CCCI 0159 PRV

NEXT GENERATION NETWORK ARCHITECTURE (NGNA)

1.0 Summary

1.1 Background

The present invention defines a network architecture for future cable industry market and business requirements. An Integrated Multimedia Architecture is described herein that cable operators and equipment vendors may elect to follow in making network and product investment decisions. A cost-efficient platform is defined with capacity and flexibility to support growth of on-demand video, high definition digital TV, managed home networks connecting a wide range of consumer-provided devices, and future IP multimedia services including IP voice, video telephony, and multiplayer gaming. These capabilities can be provided without further rebuilds of the cable hybrid-fiber-coax (HFC) networks.

One objective is to encourage broader involvement by equipment suppliers, hence stimulating more product innovation and cost reductions, through adoption of open and non-proprietary interfaces, processes, and network elements. The present invention supports retail sale of cable customer premises equipment (CPE) to consumers and allows increased flexibility by cable operators in selecting suppliers of core cable network functions.

1.2 Network architecture requirements

Cable TV operators recently completed substantial rebuilding of their HFC networks with deployed bandwidth now generally up to and above 750MHz and fiber installed deep in the plant down to nodes of 500 homes or fewer. These network investments enable cable operators to compete successfully with digital DBS providers and telephone companies, to expand consumers' choices for cable-provided services, and to increase revenues from subscribers to multiple services. Building on the industry's existing highly flexible HFC plant, the present invention has identified enhancements to the current architecture that will help to meet future business and market requirements. Such requirements are summarized in Figure 1 shown below:

Figure 1. Business and market requirements

- Expanded capacity
- Solutions based on open standards or economically licensable terms
- Exploit existing assets
- Secure rights management
- Network resource sharing
- Managed subscriber devices
- Network scalability
- Cable competitiveness
- Flexible service delivery
- Alignment with external technology
- Support for retail sale of cable CPE
- Minimized operations burden
- Support for authorized 3rd party use
- Satisfy performance criteria
- Alignment with MSO financial objectives

Although implementation of the next generation architecture will undoubtedly require trade-offs among some of these requirements, they will continue to serve as important evaluation criteria. More details on these requirements can be found in Appendix B.

1.3 Integrated Multimedia Architecture

The following are attributes of the Integrated Multimedia Architecture:

- ***Expanded capacity***. Provides expanded capacity that is non-limiting to introduction of new services. Enables cable operator options to use spectrum more efficiently through use of: analog channels for digitally-compressed video services; advanced compression algorithms; more advanced modulation schemes; integrated spectrum resource management at the head-end; and switched digital video.

- ***All-digital transition***. Supports transition to all-digital services while continuing economically to support legacy analog TVs and VCRs.

- ***Flexible, secure conditional access (CA)***. Implements CA through internal hardware (the NGNA Configurable Security Processor, or NCSP) that can be remotely configured or renewed by software downloads. Supports multiple CA options including legacy CA and new proprietary or non-proprietary CA, thus enabling integration of CPE from multiple suppliers. Provides flexibility at lower cost than physically removable CA. At the same time, cable networks can continue to support physically separable security via use of CableCARD™.

- ***Support for retail distribution***. Facilitates retail sale of subscriber video devices (SVDs) by providing capability for subscriber activation, supported by remote configuration by the operator for compatibility with any NGNA cable system.

- ***Secure in-home networking***. Supports open home networking technologies and standards, digital rights management (DRM) systems, and ubiquitous use of IP (Internet Protocol) for distribution of content in the home. Enables MSOs to offer head-end managed multi-media home network services. Supports use of multi-room entertainment systems that employ in-home storage devices to serve content to a variety of low- and higher-end networked devices. Integrates multimedia services between formerly video-centric set-top devices and data-centric PCs.

- ***Secure two-way authenticated channels via DOCSIS***. With DOCSIS 2.0 in all next generation CPE, provides secure 2-way authenticated communication channels between the head-end and CPE. This increases security relative to achievable security in one-way systems. Such channels are used for renewable conditional access key management, remote management of CPE, downloadable firmware updates, private interactive application data, and reconfiguration of encryption algorithms.

- ***Flexible transport options***: Supports broadcast, multicast and/or IP unicast video transport.
- ***CPE equipped for future transmission and compression standards***. Allows for future increases in effective system capacity with minimal incremental investment

without stranding prior CPE investments, whether such investments are made by operators or by consumers at retail.

- ➢ ***Well-defined applications environment in CPE.*** Includes capability for OpenCable Applications Platform (OCAP) middleware to support downloadable applications, enabling rapid service creation, innovation, and new business models, with intent to run OCAP on all SVDs. Provides cost savings of a standard platform without limiting the ability of cable operators to innovate in the user interface and overall look-and-feel of services.

- ➢ ***Rapid provisioning of new services.*** Supports self-installation and rapid provisioning of new services through auto-discovery, remote management, and remote configuration features of NGNA-compliant CPE.

- ➢ ***Improved resource management through open head-end interfaces.*** Restructuring of head-end network elements with open interfaces allows more efficient use of system resources, effectively increasing usable system capacity and flexibility, reducing cost, and expanding the number of suppliers of head-end components, while ensuring interconnection capability.

1.4 Specifications

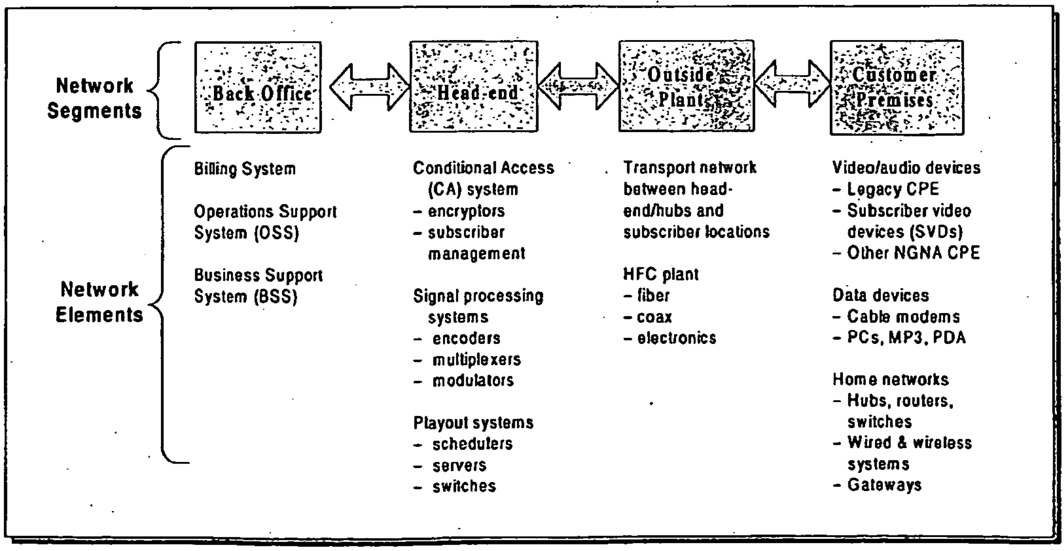
The present invention builds on OpenCable™, PacketCable™, CableHome™ and DOCSIS®.

2.0 Integrated Multimedia Architecture

2.1 Reference Architecture Description

The reference architecture is defined in terms of a set of network elements that are used to meet specific requirements. These network elements operate within the major network segments comprising the back-office, head-end, outside plant, and customer premises, as diagrammed in Figure 2 below.

Figure 2. Major Network Segments and Elements



2.1.1 Scope of NGNA architecture

The NGNA architecture of the present invention relates primarily to the head-end, outside plant and customer premises network segments, as well as to the interfaces between each of these segments and between the head-end and the back office.

2.1.2 Regulatory Requirements

The NGNA architecture is intended to be consistent with regulatory requirements for the retail availability of navigation devices and for support of CableCARD-enabled devices. One core objective is to support a new generation of retail consumer electronics equipment that will work seamlessly in providing cable services along with legacy cable equipment and new MSO-provided CPE. The NGNA architecture provides consumer electronic equipment vendors with the option of augmenting the internal NGNA configurable security processor (NCSP) by also providing a CableCARD slot. Devices with this feature will default to the NCSP when the CableCARD slot is empty; the cable operator can activate a shift to CableCARD from the NCSP after the CableCARD is inserted.

2.2 Attributes of an Integrated Multimedia Architecture

2.2.1 Video services architecture

At minimum, NGNA-compliant CPE should have the following attributes:

- ➢ *Conditional Access*. Employs re-configurable internal CA based on a hybrid of a hardware engine for decryption and software-defined key exchange. Supports multi-stream decryption for DVR, local advertising insertion capabilities and other applications requiring multiple signals.

- ➢ *DOCSIS Signaling*. All NGNA devices are two-way, using mature low cost DOCSIS 2.0 technology as foundation for two-way communications.

- ➢ *Video Transport*. Supports three modes:
  - baseline MPEG over QAM,
  - MPEG on DOCSIS convergence sublayer, and
  - MPEG encapsulated inside IP (over DOCSIS).

- ➢ V*ideo Device Applications Support*. All video CPE have the minimum required resources (i.e. memory and processor power) to support OCAP.

- ➢ *Video Codecs*. Support for decoding of MPEG-2 plus either of two advanced codecs, H.264 (MPEG4) or Microsoft's VC-9 (SMPTE). The client device should be able to switch nearly instantaneously between the currently active advanced codec and MPEG-2. The switch between H.264 and VC-9 can be made via remote command from the head-end and need not be instantaneous.

2.2.2 IP multimedia architecture

- ➢ *Extension of CableLabs Specifications*. Sets directions to extend and adapt CableHome, PacketCable, and PacketCable Multimedia to support NGNA requirements, building on previous investments in these programs.

- *Internet Protocol.* IP selected as the basic bearer layer for all in-home network multimedia services.

- *QoS (quality of service) in IP home network.* Can conform UPnP (universal plug and play standards) and CableHome to enable remote management, provisioning, and service observation of UPnP devices on in-home networks.

- *IPv6.* Support for both IPv4 and IPv6 in all NGNA IP-connected devices, with the intent eventually to transition to IPv6.

2.2.3 In-home networking

- *In-home network domains.* Defines in-home network domains as a function of level of service and of content protection.
  - GSD (Guaranteed Service Domain): QoS managed from head-end to end device.
  - ASD (Authorized Service Domain): Content can be transferred to receiving devices that have a certified, MSO-authenticated DRM system.
  - OAD (Output Authorized Domain): Content can be transferred through a rights-managed interface from the ASD to devices with non-NGNA DRM.
  - BED (best effort domain): Connected devices outside of GSD, ASD or OAD.

  CPE may be located within any one of these domains or in multiple domains where there are overlaps.

- *USB-2 port.* Provides universal CPE connection to in-home networks. Any physical layer capable of carrying IP transparent traffic (e.g. CAT5 Ethernet) can be supported through use of an adapter between the USB port and the specific physical layer.

- *Applications sharing*: Supports applications sharing between OCAP devices as well as non-OCAP devices that adhere to NGNA in-home networking standards, for example, a PC with an NGNA-compatible client. Applications examples include: remote access to DVR content; multiplayer games; personal information manager (e.g. family calendar, address book, alarm clock).

2.2.4 Advanced digital advertising

- *Advanced digital advertising.* Defines functional requirements to support advanced advertising business models including non-linear on-demand and DVR-based advertising. Requirements include support for audience measurement systems while respecting privacy, extension of DRM to monitor and control display of commercial content, extension of OCAP triggers, and capability of CA system & advanced codec to support seamless splicing of commercial content.

2.2.5 Network segment: Customer premises

- *Subscriber Video Devices (SVDs).* SVDs are NGNA-compliant video devices that include a tuner, such as set-top or set-back units or standalone digital TV sets (DTVs). A baseline (low end) SVD is defined with minimum required NGNA functionality. Higher-end SVDs include various step-up options at the discretion of suppliers, MSOs, and retailers. Baseline SVD functions and examples of step-up options are listed in the following table.

Table 1. Baseline and Extended SVD Functionality

Baseline SVD Functionality	Optional "step-up" SVD Functions (examples)
• Dual tuners, either one capable of supporting any NGNA video transport mode or DOCSIS • Two-way (reverse path) via DOCSIS 2.0 • Support for multiple transport modes • Support for decoding MPEG2 (SD and HD) plus either of two advanced codecs, H.264 or VC9 • In-home networking connectivity as a client • NGNA internal CA • Capability for OCAP middleware • Standard definition output • Analog RF output interface copy protected with Macrovision, or an approved digital interface • OEM provided universal remote control capable of controlling the SVD and the legacy TV • Frequency plan to facilitate future mid-split: upstream 10MHz to 85MHz and downstream from 88MHz to high-end of 1002 MHz • Supports up to 1024 QAM downstream modulation • Includes general purpose USB-2 port for in-home networking connectivity and possible unspecified peripheral connection	• High definition output • Copy-protected digital interfaces (e.g. HAVI, DVI) in addition to baseline analog RF. • Built-in gateway (client, server, and IP address management) function between coax and non-coax in-home networks • DVR functionality • PacketCable telephony features

- ➢ *Rights management.* NGNA CPE devices respect and protect rights of content owners over the use of their high-value content.

2.2.6 Network Segment: Outside Plant

- ➢ *Mid-split plan.* Designates future changes in use of frequency spectrum. With mid-split, upstream signals will be carried at 10MHz-85MHz versus the current 5MHz-42MHz, and downstream will start at 105MHz versus the current 54MHz.

2.2.7 Network Segment: Head-end

- ➢ *Next generation head-end.* Logical partitioning of the CMTS to facilitate unbundling, providing more efficient use of network resources and flexibility to MSOs to select the best subsystems from multiple suppliers. Definition of interfaces between CMTS components and integration of these components with other parts of the head-end. Includes unbundling of the data switching portions of the CMTS from the RF modulation portions, thereby allowing for sharing of the edge QAM resources among multiple services. Supports switching of both data and RF to enhance reliability through facility redundancy.

- *QoS & Session Resource Management.* Defines logical structure and process flows associated with QoS (requests, grants, and service assurance). Coordinates and conforms head-end QoS processes associated with all resources in head-end, outside plant, and in-home network.

- *Wideband DOCSIS.* Defines requirements for wideband DOCSIS support based on the bonding of "N" DOCSIS channels to increase the data rate.

- *OSS/BSS interfaces.* Defines interfaces with back office billing system, operations support system (OSS), and business support system (BSS).

2.3 Video Services Architecture

The common features of the NGNA video services architecture include:

- **Security:** NGNA Configurable Security Processor (NCSP) manages Conditional Access (CA), copy protection, support for secure on-demand services, secure downloads, and in-home digital rights management (DRM) functions.
- **Copy Protection**: Copy protection mechanisms for delivering content across approved outputs.
- **Firmware Downloads**: Provides device configuration and CA key exchange renewability.
- **Video Transport**: Support for broadcast, multicast and unicast options over QAM, DOCSIS, or IP/QAM encapsulation.
- **Video Codecs**: Support for MPEG-2 and either of two advanced compression algorithms.
- **DOCSIS Signaling**: Employs DOCSIS throughout to facilitate remote management of devices.
- **Video Client Software Environment**: Supports OCAP in all next generation network devices that support downloadable applications, plus provides flexibility to support applications through head-end based systems.
- **Secure Software Download**: Support for installing and upgrading software applications, drivers, kernels and OCAP implementations.

The present invention encompasses subscriber video devices that might be provided by the cable operator and/or sold at retail.

2.3.1 Security

An NGNA SVD will include an internal Next-Generation Configurable Security Processor (NCSP) for managing security aspects for cable services. Security aspects can be categorized as follows, with some overlap:

- Device authentication and management;
- CA of services between the head-end and subscriber equipment;
- Secure download of firmware updates and downloadable applications;

- Copy protection;
- Authorized Service Domain security;
- DRM within devices on one or more home networks within the Authorized Service Domain.

This section provides an overview of major attributes of the NCSP. Additional details are provided in Appendix C.

The next generation security system includes three subsystems: (1) *content and key encryption/decryption*, which is hardware-based but can be remotely re-configured; (2) *key management*, which is partially software-based and thus re-definable by secure conditional access system download; (3) *authentication*, which is partially software-based and thus renewable by the secure CAS download.
These subsystems support cable operator management of the following aspects of CA:

- Remote reconfiguration of the decryption engine to support several pre-defined scrambling algorithms including commonly used legacy CA algorithms as well as new CA algorithms;
- Software-defined initial download and renewability of the CA key exchange mechanism.

In the NCSP reference system, content can be secured with either an open standard, non-proprietary CA/DRM system and/or a proprietary CA/DRM system (legacy or otherwise).

The "flexible decryption engine" in the NCSP, as shown in Figure 3 below, is configurable to support multiple algorithms. It is flexible enough to allow configuration by remote command to be compatible with the encryption algorithms used by the CA system as well as the content protection system(s). Entitlement messages and control messages are encoded and distributed over out-of-band and in-band channels to the video CPE such that keys can be securely recovered by the NCSP; this is referred to as the firmware-defined conditional access key management application.

The secure aspects of the NCSP are protected by integration on a system-on-chip (SOC) that includes a configurable decryption engine and a micro-controller for key management. The SOC includes the NCSP and decoder elements so that in-the-clear and compressed digital video never leaves the SOC. In-the-clear digital video is protected between the NCSP and the decoder elements of the SOC using simple hashing or fast cryptographic techniques.

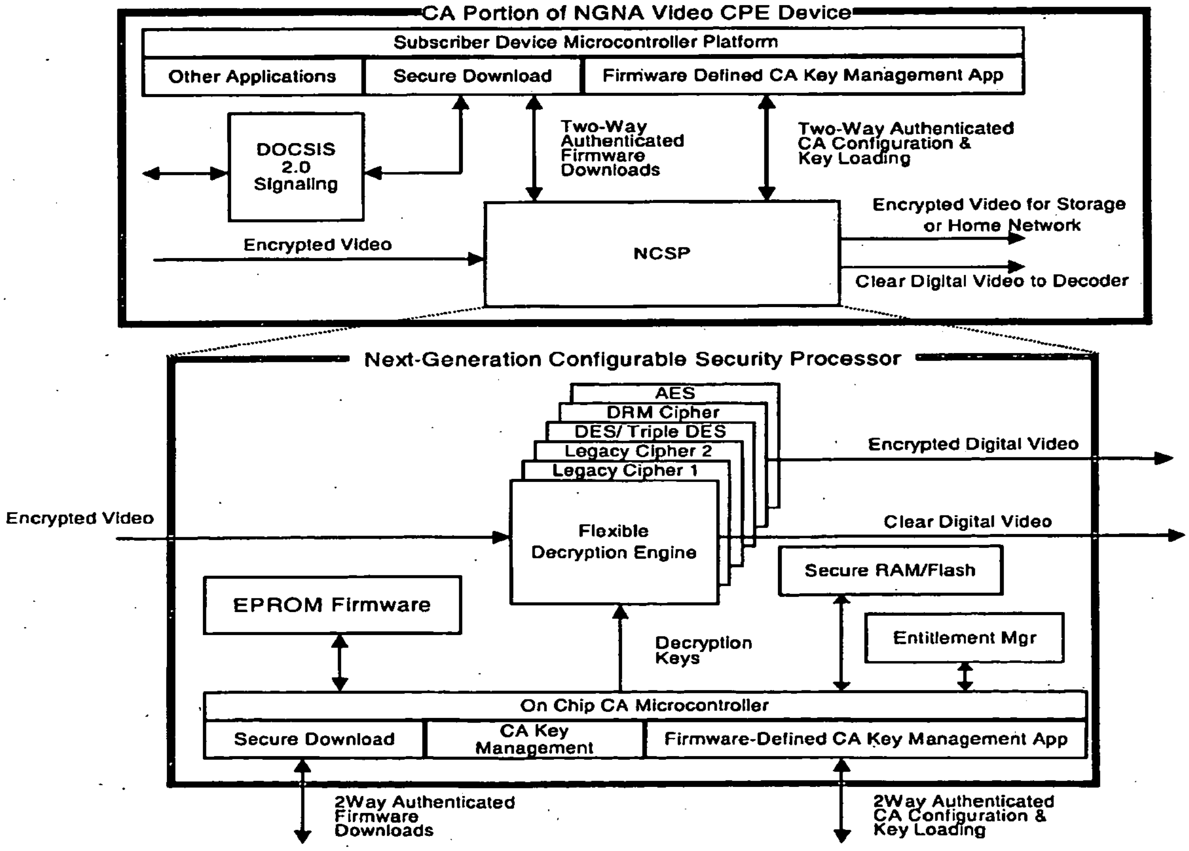
Examples of possible algorithm choices are shown in Figure 3 below. To support transition from legacy CA, the client device should possess the ability to operate in a simulcrypt or multicrypt environment. In the event that simulcrypt is enabled, the NCSP will support key sharing in the CPE.

The NCSP employs technologies to support the decryption of common proprietary and non-proprietary secure transport streams based on variants of DES, 3-DES, CSA and AES encryption algorithms. AES-128 is the preferred cipher and should be used for all future content encryption implementations. Triple DES may be used in the near term, particularly for storage of content onto CPE hard disc drives. DVB-CSA may be used as an effective transition algorithm in the near term to arrive at the AES end goal.

The NCSP is capable of securely generating digital signatures inside tamper resistant hardware without exposing the private keys or the processing needed to generate the hash and encryption keys. The next generation network is capable of digitally signing messages used for authentication and providing integrity using a secure hash.

Each NCSP in a CPE device is identified with a completely unique ID. For private serialization, each could contain a unique identifier known as a Private Seed ID. This Seed ID is used to generate the unique key to decrypt the entitlements for that specific CPE device. The CPE device is capable of changing the Seed ID to another unique value upon secure command from the head-end. The encryption key would then be generated using this new Seed ID as a component of the key. An asymmetric key could also be used to decrypt the category key sent in the EMM (entitlement management message).

Figure 3. NGNA Security Reference Architecture


CA Portion of NGNA Video CPE Device
Subscriber Device Microcontroller Platform
Other Applications
Secure Download
Firmware Defined CA Key Management App
DOCSIS 2.0 Signaling
Two-Way Authenticated Firmware Downloads
Two-Way Authenticated CA Configuration & Key Loading
Encrypted Video for Storage or Home Network
Encrypted Video
NCSP
Clear Digital Video to Decoder
Next-Generation Configurable Security Processor
AES
DRM Cipher
DES/Triple DES
Legacy Cipher 2
Legacy Cipher 1
Encrypted Digital Video
Encrypted Video
Flexible Decryption Engine
Clear Digital Video
Secure RAM/Flash
EPROM Firmware
Decryption Keys
Entitlement Mgr
On Chip CA Microcontroller
Secure Download
CA Key Management
Firmware-Defined CA Key Management App
2Way Authenticated Firmware Downloads
2Way Authenticated CA Configuration & Key Loading

2.3.1.1 Multiple Stream Support

NCSPs are capable of decrypting/re-encrypting multiple content streams simultaneously. It is expected that different NCSPs will be capable of processing differing numbers of streams depending on the capabilities of the associated CPE, but that all NCSPs will be capable of processing some minimum number of streams simultaneously. NCSPs should support the following multi-stream scenarios:

- *Watch and Record*: The ability, using two tuners, to watch one encrypted stream 'live', while recording another simultaneously to a hard drive. This likely requires the NCSP to remove the network CA encryption and apply a local hard drive encryption simultaneously to both streams.
- *Advanced Advertising*: The ability to splice two encrypted streams together, for example to replace an encrypted ad in a broadcast stream with an encrypted ad previously cached on the local hard drive.
- *DVR Server*: DVR device with multiple tuners and a hard drive that supports other devices in the home that do not have hard drives by delivering recorded material via the home network. A DVR server can support multiple concurrent record-and-play streams, e.g., streaming content concurrently to multiple devices in the home while simultaneously recording several programs. The DVR device's NCSP may have to support Watch and Record while also serving encrypted streams from the hard drive to remote devices in a multi-room DVR scenario.

NCSPs can support multiple streams by employing multiple NCSP cores, or by increasing the throughput of a single core, or both.

2.3.1.2 Conditional Access

The NGNA of the present invention envisions providing support for multiple conditional access (CA) options for the cable operator, allowing an MSO to support proprietary CA as well as any new standardized CA systems. The NCSP within each CPE can be configured to run the particular CA chosen by the cable operator.

Because the CA choice can be made anytime under control of a head-end command, a system equipped with a NCSP can be migrated gracefully from one CA option to another. The NCSP is compatible with CableCARDs. Subscriber devices that have CableCARD interfaces should default to the NCSP if no CableCARD is installed.

2.3.1.2.1 CA Software Renewability

Certain aspects of algorithms, key exchanges, key management, and cryptographic protocols are implemented in software or renewable firmware on the NCSP. Renewability in software is an important aspect of a strong security system and is desired in the next generation system. For cost reasons, it is desirable to use software renewability as a substitute for hardware renewability in as many situations as possible.

NGNA preferably does not support a "software-only" CA in which cryptographic functions are performed on a general-purpose processor. Hardware security elements are typically a required part of an effective security system for high-value content. Software and specialized hardware elements are complementary and may provide additional security over software or hardware-only solutions.

2.3.1.2.2 CA Hardware Renewability

Although software renewability is more cost effective and easier to implement operationally, some level of hardware renewability is desired in the technology for key management and transport decryption within the NCSP.

Hardware renewability of both key management and transport decryption can be achieved in several ways using removable hardware capable of supporting the bandwidth requirements of transport streams. For example, for NGNA devices that support a multi-stream CableCARD interface, the insertion of a CableCARD would allow full renewability. Alternatively, a communication port such as USB 2.0 could be used to host a new device that could be deployed for full hardware renewability if device security were compromised.

2.3.2 Copy Protection

If an NGNA device employs a CableCARD, the interface should implement renewability and configurability in compliance with SCTE-41 as described in Part 76 of FCC rules. Additional next generation copy protection methods are also contemplated.

2.3.3 Firmware Downloads

SVDs are assumed to support three types of secure firmware downloads:

- General control firmware that controls the user interface, device operation, and support for applications (e.g. VOD, EPG, OCAP);
- Internal firmware that manages and communicates with the NCSP;
- Highly secure messages intended to be passed to the NCSP, which reconfigure the hardware engine and/or install CA key management firmware in the NCSP.

The secure downloads are encoded for transmission to the SVD over a secure channel. All of the secure download signal paths require two-way authenticated exchanges and it is further assumed that physically accessible signals paths between blocks in Figure 3 above are encrypted.

2.3.4 Video Transport

Digital video and audio streams are typically carried over MPEG-2 transport streams. Both Single Program Transport Stream (SPTS) and Multiple Program Transport Streams (MPTS) may be delivered at various segments of the system. MPEG-2 Program Specific Information (PSI) and ATSC/SCTE defined System Information (SI) are used at the MPEG transport layer.

2.3.4.1 Backbone

The backbone audio/video transport (broadcast and on demand) is typically MPEG-2 transport over User Datagram Protocol (UDP)/IP carried over Gigabit Ethernet. Both SPTS and MPTS may be used. An example of SPTS is a Video On Demand stream at the streaming server's Gigabit Ethernet output.. An example of MPTS is the multiplexed broadcast streams from a multiplexer. The IP encapsulation in the backbone is usually terminated at the edge of the network (at the QAM or CMTS).

Future backbone networks may make use of RTP or other protocols to recover timing affected by jitter and latency in the network. The use of an additional header such as

RTP may enable additional video specific information to be carried in the packet, such as VOD session ID or program ID.

2.3.4.2 Edge to Subscriber Premises

The NGNA reference architecture contemplates three alternative means to carry audio/video data between the head-end edge (e.g., QAM or CMTS) and the subscriber premises. The video data is compressed via MPEG-2 or an advanced encoding scheme described below. Audio data is in MPEG-1 Layer3, Dolby AC-3 or an advanced audio encoding scheme. The three possible transport methods are:

- **Baseline: MPEG-2 Transport over QAM**
  MPEG-2 Multiple Program Transport Stream (MPTS) over QAM is the conventional approach used in today's digital cable system. In order to maintain backward compatibility, the digital subscriber video device (SVD), or next generation video CPE, should be able to process MPEG-2 transport over QAM for both broadcast and on demand applications. The transport stream payload may be MPEG-2 audio/video or an advanced codec compressed stream.

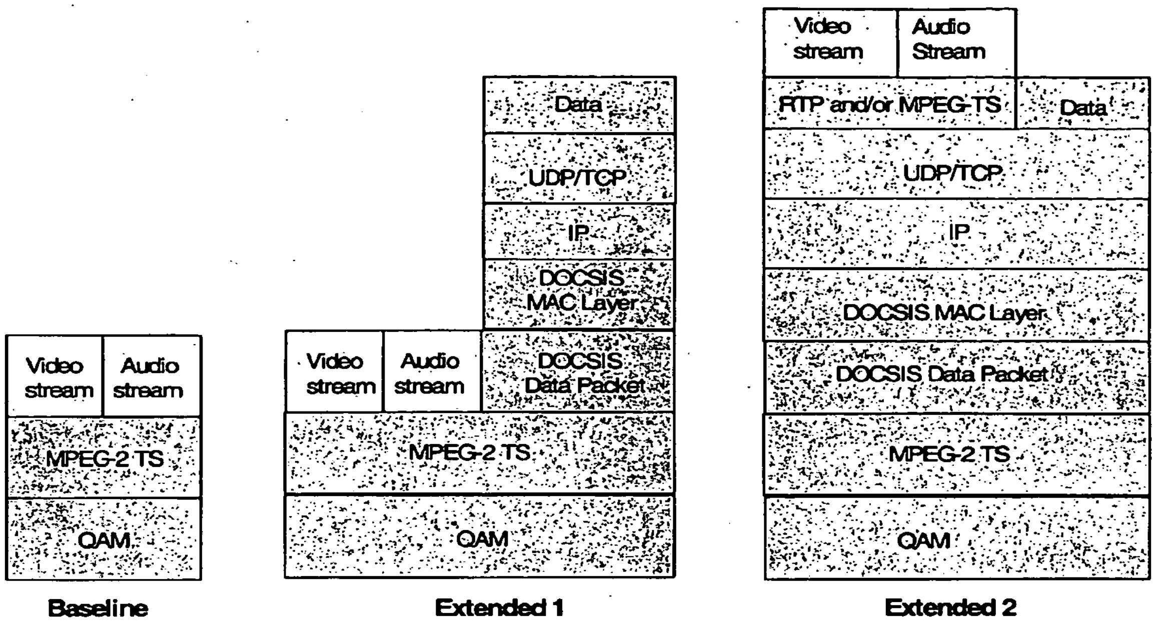
- **Extended 1: MPEG-2 Transport multiplexed with DOCSIS**
  In this approach, the MPEG-2 transport stream (DOCSIS downstream transmission convergence sub-layer) is used to multiplex audio and video program information with DOCSIS data. The well-known PID 0x1FFE is used for MPEG-2 transport packets carrying the DOCSIS payload (as defined in the DOCSIS specifications), and other PIDs are used for various audio, video and data streams. NGNA envisions that this video transport approach can be used in addition to the baseline MPEG-2 transport over QAM approach to support advanced video based multimedia services that are integrated with data over cable services.

- **Extended 2: Video over IP/DOCSIS**
  In this approach, video is carried over IP and delivered over DOCSIS channels. This allows future services such as IP based streaming media to the digital SVDs. The audio and video data may be carried in any of these formats:
  - MPEG-2 transport packets over IP over DOCSIS;
  - MPEG-2 transport packets in RTP payloads over IP over DOCSIS;
  - RTP (or other realtime IP timing protocol) payloads over IP over DOCSIS.

  The receiving CPE should be able to process streams delivered in any of the three formats.

It is preferably required that the subscriber terminal supports all three transport methods, Baseline, Extended 1, and Extended 2.

Figure 4. Alternative Video Transport Approaches



2.3.5 Video Codec

NGNA cable systems will deliver video content in either of two compressed formats: MPEG-2 (both high definition and standard definition) as delivered on today's systems, and an advanced compression format. The choice of MPEG-2 or an advanced codec will be on a program-by-program, or service-by-service basis (including switching between program and advertising content). Therefore the SVD should be able to switch rapidly between decoding MPEG-2 compressed content and advanced codec compressed content. The transition from MPEG-2 content decoding to advanced codec decoding should be as seamless to the viewer as current transitions between MPEG-2 programs.

The advanced compression format will be either H.264 (MPEG-4 Part 10 Advanced Video Coding, Main Profile, Level 3 for standard definition and Level 4 for high definition) or VC-9 (Advanced Profile, Levels for standard and high definition).

The cable operator will choose which advanced compression format to use. It is not expected that an operator will use both advanced compression formats simultaneously on the plant. Therefore the SVD is expected to be capable of decoding both MPEG-2 and only one of the advanced codecs at a time. It is expected that the SVD would discover which advanced codec is needed for the system it is attached to and configure the decoder appropriately at boot time. This could imply download of appropriate firmware or activation of the appropriate resident firmware.

In addition to advanced video coding techniques, advanced audio coding schemes with significant improvement over the currently deployed Dolby AC-3 scheme are also contemplated.

2.3.6 DOCSIS Signaling

The NGNA according to the present invention includes multiple roles for DOCSIS including secure signaling for all CPE and alternative transport of video. For multimedia services, DOCSIS supports streaming media for which QoS is an important factor. DOCSIS transport and DOCSIS set-top gateway (DSG) protocols support secure software download and remote configuration management of SVD subsystems enabling:

- Configuration of the NCSP;
- Download of renewable firmware for basic control of the devices;
- Remote configuration of the video decoder algorithm;
- Download of applications designed to run on OCAP middleware; and
- Session management traffic for interactive content such as VCR-like controls for VOD.

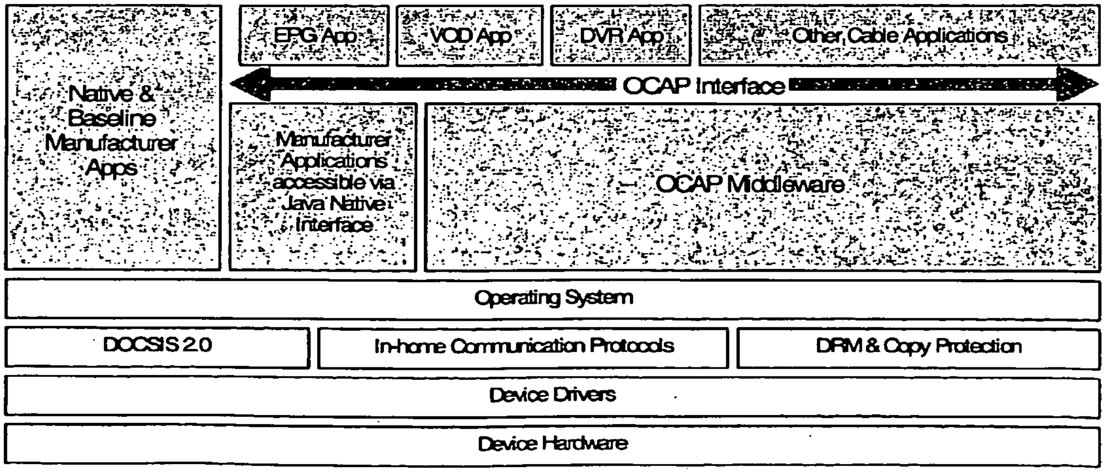
Important additional benefits of employing DOCSIS are its native features for remote management from customer support systems and operation support systems. Consistent with CableLabs' CableHome™ initiative, this capability allows all CPE to be visible from the head-end.

2.3.7 Video Client Software Environment

All NGNA-compliant SVDs are provided with sufficient memory and processor resources to be capable of running the OCAP middleware (OCAP version 1.0 at a minimum). The middleware may be resident or downloaded to the device. OCAP provides a consistent environment for unbound and bound applications; the former (unbound applications) are independent of any particular programming channels, such as a game, and the latter (bound applications) are tied to specific programming channels such as a clickable link to a review of a movie currently being watched.

OCAP comprises a set of APIs for the middleware component of a software solution. OCAP specifies a set of permission request files, a digitally signed code image and a monitor application for various security and resource contention issues. Figure 5 describes the software architecture in video CPE hosting OCAP.

Figure 5. Video CPE Software Architecture



The present invention identifies two categories of native applications that the device manufacturer would likely include in its products. Manufacturer applications described as "native and baseline" would have direct access to the operating system and bypass the OCAP layer to interface directly to host and user interface; for example, these might include giving the user the ability to select between cable-ready versus off-the-air broadcast mode of operation. The other category of manufacturer applications is designated as "accessible via Java Native Interface" (JNI). These applications would also be supplied by the manufacturer and would map through the OCAP middleware layer.

The default for OCAP is to pass these applications through to the host and user interface; however, OCAP has the ability to modify the default or even to supplant the OEM application with a new application, for example, by one downloaded by an end-user on top of OCAP. An example of such default native applications might be up/down control of the sound volume on a DTV. Normally OCAP would allow the manufacturer's application to have control, but in the event of an emergency alert (EA), the MSO EA application running on top of OCAP could take over control of the sound volume.

Downloadable applications run in the OCAP middleware environment. Examples of applications that an MSO may choose to download would most likely include a core set of essential applications: electronic program guide (EPG), video on demand (VOD), and other cable applications such as support for head-end rendered applications. With this last option, the visual display of the user output interface is created as a still video frame picture at the head-end for freeze frame display by the CPE, or alternatively this may be implemented as a unicast video stream if bandwidth allows and the user interface involves moving components. Support for the user input interface can include relaying user interaction with the remote control back to the head end to communicate a menu selection, or cursor selection, from the display.

There are expected to be differences between CPE devices in terms of applications and capabilities that are supported. For example, high-end devices will support some applications, such as DVR, that are not present on lower-end CPE.

2.3.7.1 Security Enhancements

Next generation client software is an important component in the overall system security architecture. Since system security for boot-time authentication, device driver authentication and system kernel security may not be covered in the OCAP specification, it is important to specify the other security requirements for the complete next generation client software solution. The suggested solution includes a trusted and non-modifiable boot loader that is the foundation of all software downloads and upgrades. It also includes the authentication of all software elements including OCAP implementation, system kernel, device drivers, OCAP applications and all other software at both boot time and during download. In addition, it includes trusted kernel technology that creates a trusted environment for task context switching. All cable-provided client software security in the CPE should be tied to the trust of the CA system instead of creating a separate standalone trust model.

2.3.7.2 Advanced User Interface

OCAP and head-end based applications can be employed together with other NGNA elements to provide advanced user interfaces to new services. Since the next generation network architecture supports a much richer variety of services as well as rapid service introduction, it is important to have intuitive user interfaces that are convenient and easy to learn to use.

The NGNA of the present invention is intended to support expanded hardware and software user interface concepts beyond baseline remote control keypads and/or keyboards such as:

- Advanced remote controls with new input devices such as touch pads, pointing devices, and software defined keypads;
- Remote controls, or other ancillary devices with screens additional to the main display screen that allow messages, web pages, navigation, help, or control information to be displayed to one person or multiple persons in the same room;
- Non-typical input/output devices such as force feedback on game controls, vibration devices keyed to program content, and special effects generators that present three-dimensional sound effects.

In order to support such additions, a standard expansion port is defined (see Customer Premises section below) that can be employed to interface to an external advanced user interface device.

2.4 IP Multimedia Services Architecture

Core IP multimedia services include high-speed data service and VoIP-based telephony, the former based on technologies developed on the DOCSIS project at CableLabs, while the VoIP architecture has been specified under the PacketCable umbrella. It is anticipated that cable-provided interactive IP-based multimedia offerings will grow to include, as representative examples: the sharing and display of high-quality still photographs, full-motion video telephony and conferencing, presence-enhancement for emerging communications media, applications-sharing and collaboration tools, and online-enabled multiplayer gaming. The next generation IP multimedia services architecture will serve as an enabling platform for a rich suite of applications addressing a wider range of CPE devices and a richer set of services.

Many IP multimedia services are sensitive to network latency, jitter and throughput; the NGNA enables end-to-end QoS treatment for data traffic associated with IP multimedia services delivered to devices within in-home network domains. In addition to supporting QoS, it provides for service provisioning and monitoring, digital rights management, and NAT-traversal.

IP multimedia services are delivered over IP transparent channels, both (i) between the head-end and subscriber premises and (ii) within in-home network domains involving protected content (Authorized Service Domain, or ASD) and managed QoS (Guaranteed Service Domain, or GSD). Physical network layers could include IP traffic on coax or non-coax in-home networks, e.g., CAT5, HomePlug, or wireless. While NGNA for different types of services could support essentially any physical layers, in general there is a preference for PHY layers that support QoS and offer capacity for multiple HD channels.

Potential IP multimedia service endpoints might include OCAP subscriber devices connected to the coax network, PCs sharing a DOCSIS high-speed data connection over the in-home data network, and personal wireless devices providing mobility and convenience functions within the home. A sampling of prospective IP multimedia applications hosted on these CPE follows:

- PC(s) on the in-home IP data network configured as media servers and accessed by subscriber video CPE on the in-home IP network for high-fidelity presentation of music, video, or still pictures;
- Gaming consoles interfacing with both video CPE and the home and access data networks facilitating participating in online multiplayer gaming sessions;
- Video telephony terminals and mobile, wireless communications devices receiving enhanced QoS-based network support while sharing infrastructure with other services within the home;
- Internet appliances that provide for telephone caller ID display, call logging, and message retrieval on subscriber video devices and PCs.

NGNA supports extensions to the cable network that will enable cable operators to partner and/or compete with wireless voice and data service providers, offering services such as:

- Unified messaging services that integrate wireline with wireless universal numbering, voicemail, fax, follow-me voice, email, rich media messaging, and virtual private networks;
- IP mobility and roaming between cable modem services and public network WiFi hotspots;
- Deploying access points on outside plant to provide WiFi or other wireless technology coverage in public locations.

2.4.1 Transport

The delivery of Multimedia Services will be over IPv4 using both unicast and multicast. Support for IPv6 will be necessary to ensure future capabilities of the NGNA as more network devices are connected to the network.

The regional area network will be IP-based and is anticipated to be carried over Gigabit Ethernet technologies, e.g., 1GigE and 10GigE. It is likely that a common regional area network infrastructure will be shared between the video and IP multimedia services architectures.

In the HFC access network, the reference architecture calls for the use of DOCSIS as the underlying transport mechanism.

The NGNA of the present invention does not prescribe specific in-home data network physical layers (PHY). However, any suitable PHY should satisfy two requirements:

- The PHY should provide IP transparency for services in all in-home network domains.
- For services within the in-home network domain involving QoS, the PHY should also be capable of being QoS-managed.

Subscribers may select any of a number of choices that are IP-transparent. However, PHY/MAC combinations that can be QoS-managed by NGNA protocols will provide a better user experience. Also, not all PHY choices will have capability to support high bandwidth applications such as multiple HD streams. Examples of IP-transparent PHY that might be used with NGNA systems include WiFi 802.11a/b/g, HomePlug, HomePNA, MoCA, and CAT5 wiring.

2.4.2 End-to-End Quality of Service

The overall experience that a user will enjoy is dependent upon the end-to-end treatment that a network service's traffic receives. Consequently, it is important to address the boundary between network segments to ensure that appropriate coordination is provided in managing overall session quality.

One approach is to distinguish three broad segments of the network: the Regional Area Network (RAN), defined as the core network consisting of the bridge between the source of the content or service and the access network; the access network, defined as the HFC segment connecting the CMTS and cable modem (CM) elements; and finally the home network, broadly defined as the entire (physical-layer-agnostic) network topology behind the CM within the home.

The NGNA incorporates by reference the mechanisms developed at CableLabs under the PacketCable and CableHome projects; PacketCable Multimedia (PCMM) focuses on the access segment, while CableHome targets the home network segment. In addition, the NGNA defines a bridge or gateway between the in-home coax network (typically an extension from the coax drop that connects to TVs and other video devices inside the home), and in-home data networks (typically subscriber-owned, often other than coax, that support PC-centric applications).

2.4.2.1 Regional Area Network QoS

Many Regional Area Networks (RANs) are maturing to distinguish and route packets over divergent paths (with associated quality metrics) based upon packet marking. PacketCable Multimedia, in conjunction with DOCSIS, supports DiffServ strategies on the RAN by allowing the MSO to associate a particular DiffServ Code Point (DSCP) with each upstream service flow. All packets exiting this flow will be tagged with this DSCP before entering the RAN. Similarly, PacketCable Multimedia includes the capability to distinguish incoming downstream traffic received from the RAN and to place this traffic on an appropriate service flow based on DSCP markings (as well as conventional IP and MAC-layer originating and terminating address mechanisms).

The respective architecture has been outlined in the PacketCable Inter-Domain QoS specification that can be found at:
http://www.packetcable.com/specifications/specifications12.html

Although network architectures outside of RANs are not discussed herein, there are recognized potential benefits of standards for traffic peering for content and services beyond the current peering arrangements for HSD traffic. For example, the ability to keep VOIP calls "on-net" end-to-end could provide significant cost savings. This is especially true in geographic areas where cable operators have adjacent RANs. Such peering arrangements would include hardware and protocol interfaces and suitable "settlement" systems.

2.4.2.2 Access Network QoS

The PacketCable Multimedia (PCMM) specification defines an application-agnostic technology framework for providing session-based dynamic QoS-enhanced network services over a DOCSIS 1.1 (or later) access segment.

A prerequisite to the deployment of the PacketCable Multimedia framework is the availability of a DOCSIS 1.1 (or later) segment. DOCSIS 1.1 added MAC-layer support for Dynamic QoS. To facilitate the delivery of multimedia sessions requiring QoS guarantees, the PCMM framework leverages these DOCSIS mechanisms and expands upon the architecture to support general-purpose Dynamic QoS functionality based on mechanisms defined in the core DOCSIS 1.1 and PacketCable 1.x voice specifications. While PacketCable Multimedia is based on mechanisms defined in PacketCable 1.x, it is important to note that a pure PacketCable Multimedia deployment requires no PacketCable 1.x network elements.

Several network elements and interfaces have been identified and profiled within the PacketCable Multimedia specification (available at http://www.packetcable.com/specifications/multimedia.html).

While no session establishment protocol is defined in PacketCable Multimedia (i.e. it is application agnostic), the NGNA recognizes the prevalence of SIP in many of today's multimedia applications. One of the goals of the architecture is to support a wide variety of applications and their associated session establishment mechanisms. The NGNA will implicitly support SIP in addition to other application-specific session establishment mechanisms.

SIP-based applications can take advantage of access QoS in one of two ways. For basic QoS-unaware devices, it may employ a 'push' QoS model where the SIP Proxy server makes a QoS request for access resources on the client's behalf. An alternative approach is to employ a 'pull' model where the SIP client contains more intelligence and requests its own access resources (pulling them from the network). Both of these approaches are currently defined in the PacketCable Multimedia Architecture Framework document (http://www.packetcable.com/specifications/multimedia.html). While the 'push' method is currently supported by the PacketCable Multimedia specification, the 'pull' method is not. The 'pull' method will be introduced when in-home and access QoS are bridged via UPnP.

2.4.2.3 In-Home Network QoS

CableHome specifications are intended to provide Internet Protocol (IP) - based architecture for managed home-networked services on the cable network through a DOCSIS cable modem.

NGNA in-home network architecture is partly defined by existing aspects of CableHome 1.1 specifications. However the current version of CableHome 1.1 only includes prioritized QoS across the home network to devices that include CableHome QoS boundary point software. In order to fully support NGNA QoS objectives, CableHome 1.1 needs to be extended to provide for parameterized QoS control by bridging UPnP and PacketCable Multimedia.

QoS capabilities may or may not be provided to the end client, depending upon the layer-two technologies employed and the location of the client in the network. From a QoS perspective, the client can reside in one of two in-home network domains, in the Guaranteed Service Domain (GSD) or outside the GSD. When a client resides in the GSD, it has QoS capabilities at its disposal for establishing not only in-home network QoS, but also bridging the in-home QoS to the access network for end-to-end QoS treatment. For clients outside the GSD, in-home QoS is not available; however, the client may still receive access and RAN QoS treatment through application level signaling. This type of client is most likely a legacy QoS unaware device that can still benefit from access level QoS treatment.

To bridge between the access and in-home networks, the CableHome device can take advantage of the robust packet classification mechanisms introduced in DOCSIS 1.1 and carried on into PacketCable Multimedia. It is possible to identify and forward packets exiting the home network segment based on a number of distinguishing characteristics, including IP and MAC-layer originating and terminating addresses and ports, DiffServ/TOS marking and 802.1q VLAN tags.

Currently CableHome 1.1 has adopted a packet marking and priority queuing scheme based on 802.1q. Moving forward, alignment between CableHome QoS capabilities and those defined by UPnP is anticipated.

For devices to reside in the GSD, the home network links between the gateway and GSD device should support parametric QoS. Additionally, the client device should comply with CableHome Quality Boundary Point requirements (which are a superset of UPnP Device requirements).

NGNA provides application level interfaces allowing client services to request bandwidth and content resources. The specific network segment within which these resources reside will determine what interface which will be accessed. It is desirable to maintain a common language in order to simplify application requirements. Examples of these interfaces may include Packet Cable Multimedia with SOAP/XML extensions, CableHome with UPnP QoS support, and OCAP Home Networking Application extensions. These enhancements provide a standard mechanism for application interface.

2.4.3 Telemetry Services

It is anticipated that next generation networks will support telemetry and control applications such as home security, remote health monitoring, and energy management. These services could be deployed to any home passed by the cable infrastructure, regardless of a home's current subscription status. The network should be able to support potentially large-scale deployments of endpoints that receive a constrained service set. To illustrate this further, consider the example of a remote meter reading service customized for use with a contracting utility. The meter would generate very low rate IP telemetry that could be carried over the broadband network from the source in the home (the electric meter) to the data aggregator (within the utilities' domain). The system will restrict data flows to those required for the application (in this case the electric meter and the data aggregation server) and prevent any unauthorized use of the network. The cable operator would ensure a monitored and robust connection to bring the meter data to the utility. The utility would deploy the equipment to every home in a geographic area.

2.4.3.1 IPv6

In order to support the envisioned large-scale deployments, support for IPv6 is necessary for DOCSIS based network clients (telemetry devices with an embedded DOCSIS CM). This requirement is necessary to ensure capital investment is not stranded and to ensure a large enough address space to support utility-based telemetry services in addition to other smaller market services. While co-existence and transition strategies for IPv6 have not yet been defined, support for IPv6 can be interpreted as software upgradeable. No hardware upgrades should be necessary to support IPv6 for NGNA devices (this may or may not be true for existing legacy devices).

2.4.3.2 Security and Privacy

In order to provide a telemetry service, consideration of the user's privacy and thus the securing of the user's data are important. NGNA provides mechanisms to allow an endpoint to authenticate the request as well as secure the endpoint's response to such requests. The following features are required for secure telemetry and control applications:

- All endpoints should have factory defined identities;
- Secure cryptography mechanisms (i.e. AES, 3DES) should be maintained through all tuning, gateway, network and client elements; and
- All management communications (XML, SNMP) should be able to be secured.

2.5 In-home Network Architecture

This section is about "in-home networking" within and between the several networks that will exist within the home.

While many homes have one or more home networks today, they are generally not well integrated with the cable system and provide limited support for multimedia (e.g., best-effort delivery of low-quality video vs. guaranteed delivery of HD video.) Extension of cable operator-provided services and content onto home networks will enable a greater variety of devices to participate and provide new opportunities for novel services and business models.

The next generation network architecture includes a comprehensive in-home network architecture that supports the seamless transfer of traffic between devices on the cable outside plant (e.g., DOCSIS, MPEG-TS) and various home network segments/technologies. NGNA supports a variety of application models within the in-home network. One such aspect has OCAP on both client and server devices (e.g., a low-end SVD communicating with a high-end SVD). In addition, NGNA can also define application interfaces, such as UPnP Remote UI, that are independent of the OS and middleware on certain devices.

Examples of services and applications that such an in-home networking architecture support include:

- A low end subscriber video device (SVD) could access a high end SVD functioning as a digital video recorder (DVR) on the coax network for the purpose of viewing content stored on the hard drive of the high-end SVD. Thus, the low-end SVD would access the DVR application function of the high-end device without the cost of an additional hard drive and also provide a unified view of stored content at multiple locations in the home.

- A low-end SVD with limited memory and processing power could access OCAP supported applications running on a high-end SVD and obtain the application functionality as though the application were resident on the low-end SVD.

- An SVD on the coax in-home network could access video or multimedia media content resident on a personal computer located on the non-coax in-home network, or vice versa.

- Message traffic could be passed between the in-home coax and non-coax network to support applications such as display of caller ID on TV connected to an SVD or perhaps display of the e-mail inbox summary on a TV connected to an SVD.

The most demanding traffic on the in-home network in terms of bandwidth is likely to be high definition TV (HDTV) content; MPEG-2 based HDTV content can use up to 12Mbps-19Mbps of bandwidth for a single program. There is a preference for PHY layers that provide capacity for simultaneous real-time streaming of multiple HDTV channels within and between various in-home network segments and technologies.

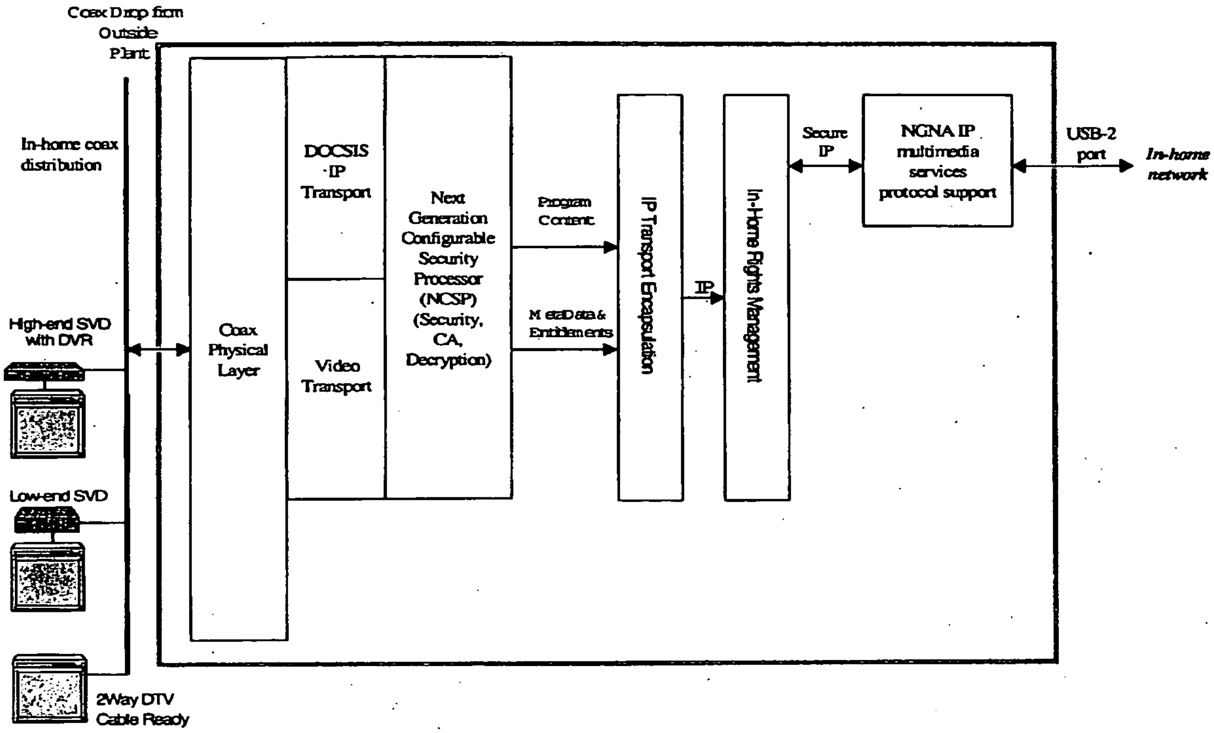
The CableHome project has defined a home networking gateway element to bridge between the cable operator's DOCSIS network and the subscriber's in-home network(s). This gateway is designed to be provisioned and managed in a secure fashion, and additionally can prioritize packets passing between the DOCSIS and home network segments. The next generation in-home network architecture complements the foundation elements defined by the CableHome project with the considerations necessary to transport high quality content (e.g., content requiring rights management and stringent QoS enforcement) within and between each network, to manage various LAN segments, and to admit client devices to the network.

2.5.1 General Architecture Elements and Domains

A gateway element extends the functionality of CableHome Portal Services (PS). This gateway element adapts the in-home network segment(s) to the DOCSIS, and possibly MPEG-TS, network; its functionality includes transferring traffic among and between various in-home network segments(s) and technologies. The gateway can have many physical implementations, from embedded cable modems, to modem/NAT combinations, to implementations within a high-end SVD.

As shown in Figure 6, the gateway provides the ability to support multiple transport technologies allowing traffic to move seamlessly around the premises in a transport-agnostic IP environment. The traffic on the in-home network may comprise various combinations of content, content control, navigation, and applications sharing to allow for interaction between data, video, and IP multimedia services.

Figure 6. Gateway Communications Architecture

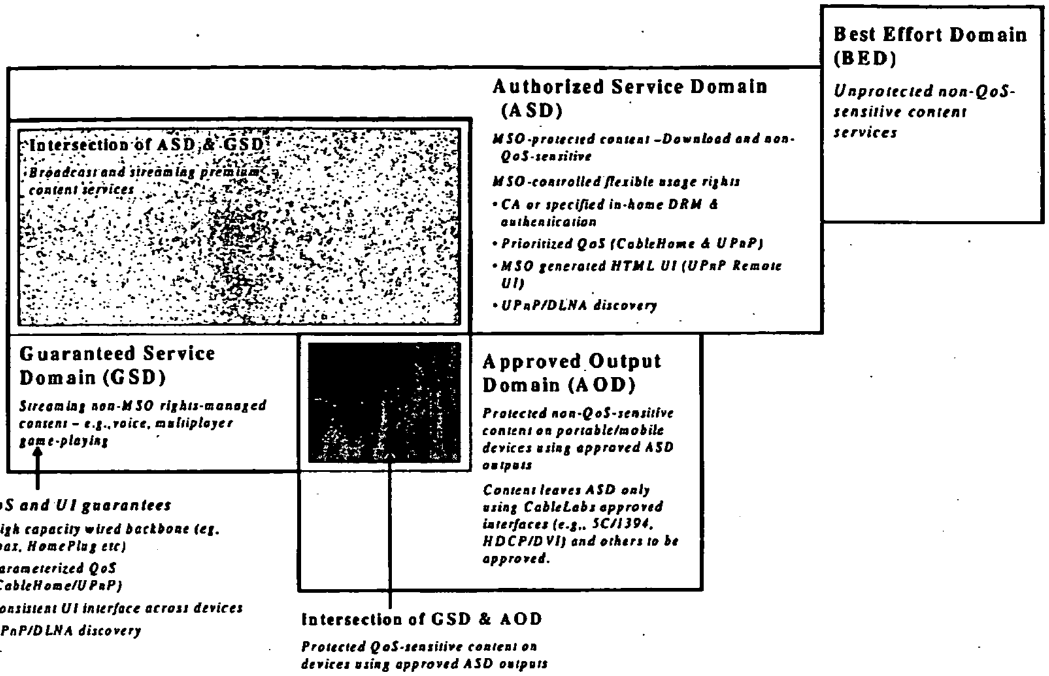

Coax Drop from Outside Plant
In-home coax distribution
High-end SVD with DVR
Low-end SVD
2Way DTV Cable Ready
Coax Physical Layer
DOCSIS IP Transport
Video Transport
Next Generation Configurable Security Processor (NCSP) (Security, CA, Decryption)
Program Content
MetaData & Entitlements
IP Transport Encapsulation
IP
In-Home Rights Management
Secure IP
NGNA IP multimedia services protocol support
USB-2 port
In-home network

The various in-home network technologies are unspecified at the media access control (MAC) and physical layer. Candidates for these layers include any known, or future, layers capable of high-speed Internet protocol (IP) support. Examples of such layers include Ethernet over CAT5, HomePlug power line carrier, Home PNA, MoCA, and 802.11a/b/g/n. It is likely that many homes will utilize multiple home networking technologies to meet different needs.

The various in-home network segments are assumed to be IP-based; in addition to providing continued support for high-speed data applications, IP provides a standards-based and ubiquitous interoperability layer across multiple network technologies and devices.

As shown in Figure 7, within the communications architecture of the in-home network, there are functional domains that vary both by management of QoS and in terms of rights management (content protection).

Figure 7. In-Home Network Domains - Overview



Best Effort Domain (BED)

Unprotected non-QoS-sensitive content services

Authorized Service Domain (ASD)

MSO-protected content –Download and non-QoS-sensitive

MSO-controlled flexible usage rights

- *CA or specified in-home DRM & authentication*
- *Prioritized QoS (CableHome & UPnP)*
- *MSO generated HTML UI (UPnP Remote UI)*
- *UPnP/DLNA discovery*

Intersection of ASD & GSD

Broadcast and streaming premium content services

Guaranteed Service Domain (GSD)

Streaming non-MSO rights-managed content – e.g.,voice, multiplayer game-playing

Approved Output Domain (AOD)

Protected non-QoS-sensitive content on portable/mobile devices using approved ASD outputs

Content leaves ASD only using CableLabs approved interfaces (e.g., 5C/1394, HDCP/DVI) and others to be approved.

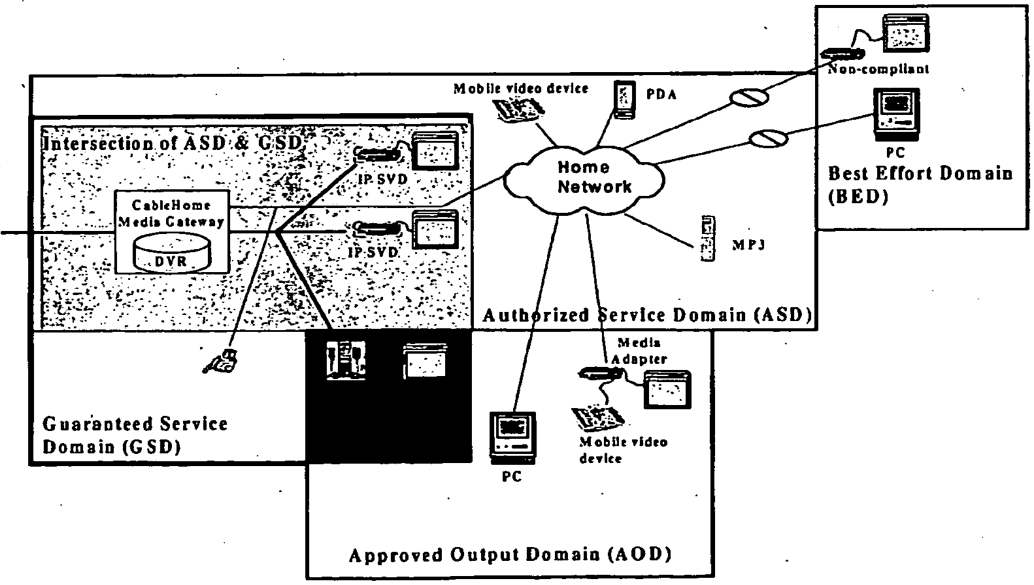
QoS and UI guarantees

- *High capacity wired backbone (eg. coax, HomePlug etc)*
- *Parameterized QoS (CableHome/UPnP)*
- *Consistent UI interface across devices*
- *UPnP/DLNA discovery*

Intersection of GSD & AOD

Protected QoS-sensitive content on devices using approved ASD outputs

Figure 8. In-home network domains - Examples



Guaranteed Service Domain (GSD)
If guarantees of QoS can be maintained from the head-end to a client, the client is considered to be part of the Guaranteed Service Domain.

In order to ensure guaranteed QoS, the client should support the appropriate QoS signaling: the home networking technology that the client is connected to should be able to provide the guarantees for the necessary QoS parameters such as bandwidth, jitter, and\ delay, and it should have enough capacity to carry multiple high-definition streams. Example technologies that in the future intend to meet these requirements are wireline technologies based on coax (MoCA), powerline (HomePlug) and phoneline (HPNA 2.0).

The home gateway should support the appropriate QoS signaling and necessary hooks to bridge in-home QoS with the access network QoS, and it should implement CableHome QoS functionality while the client device should implement UPnP QoS. The CableHome QoS functionality is a superset of UPnP QoS. Hence, a given client may be in the GSD when connected to one network segment in the home and not in the GSD when connected to another. Similarly, a given segment is likely to have some clients that are in the GSD and some that are not, based on the level of QoS support in each client device and application.

All the devices and the stored content in this domain can be discovered using a mechanism defined by UPnP/DLNA (Digital Living Network Alliance, formerly called Digital Home Working Group or DHWG). The home gateway acts as a centralized discovery server for the in-home LAN. The cable operator can access this information through a CableHome-defined MIB interface.

Devices in the GSD are able to receive QoS-sensitive content services such as VoIP, multiplayer interactive gaming, and IP Video-Phone. This content may or may not contain third-party DRM-based content protection.

Authorized Service Domain (ASD)
The devices in this domain arc able to authenticate themselves and support content usage rights as defined by the MSO. This segment includes devices that comply with the in-home digital rights management as described below.

It is not necessary to provide QoS to the devices in the ASD. However, the client devices may be able to support prioritized QoS and therefore should implement UPnP QoS signaling. The home networking technology should be able to support prioritized QoS, particularly in segments where latency- and bandwidth-sensitive content is streamed.

All the devices and the stored content in this domain can be discovered using UPnP/DLNA-defined discovery mechanism.

Devices in the ASD are able to receive protected non-QoS sensitive content services such as music and non-real-time or low bit-rate video.

Approved Output Domain (AOD)
The devices in this domain are connected to the ASD using CableLabs' approved output interfaces. When the content flows from the ASD to AOD, the MSO-specified usage rules are asserted across the interface. Currently, 5C over 1394 and HDCP over DVI (or HDMI, High Definition Multimedia Interface) are the only two approved digital output interfaces. However, under the plug-and-play agreement, more output interfaces may be submitted to CableLabs for approval or can be approved by four major studios. For example, a possible interface that may be established is a DRM interface that allows the communication of content and usage rules to a third-party DRM system, separate from the DRM of the MSO.

A cable operator relinquishes direct control over the content once it is transferred over the AOD. This is a key difference between Authorized Service Domain and Approved Output Domain.

Under the current plug-and-play agreement, a device may receive content from the ASD over an approved interface. There is no mandate that the device meet any other requirements related to QoS and device discovery. However, some AOD devices will be able to participate in the Guaranteed Service Domain as it relates to device discovery and QoS. All devices in the AOD will be able to receive protected non-QoS sensitive content that has MSO-enforced usage restrictions that depend upon the approved output interface.

Removable media such as recordable DVDs, flash cards and CD-Rs will typically be found in the AOD.

Best Effort Domain (BED)
Devices and physical layer segments not conforming to the requirements of the above three defined domains may still be discovered and participate in services that do not require content protection or guaranteed quality of service.

Intersection of GSD and ASD
The GSD and ASD are independent; a device can belong to neither, one or the other, or both. The devices that belong to both GSD and ASD can provide QoS guarantees and can authenticate themselves and support the in-home DRM. Such devices represent a higher level of compliance and may be able to receive high-value content with MSO enforced usage restrictions.

Intersection of GSD and AOD.
The GSD and AOD are independent; a device can belong to neither, one or the other, or both. The devices that belong to both GSD and AOD can provide QoS guarantees for the content that flows from ASD to AOD over approved interfaces. Such devices are able to receive protected QoS-sensitive content with MSO enforced usage restrictions depending upon the approved interface.

Exclusivity of ASD and AOD
The ASD and AOD are mutually exclusive. A device can belong to only the ASD, or AOD, or neither.

The following table summarizes various functional requirements for devices in different domains.

Table 2. Functional Requirements of Different Domains & Offered Services

Functionality*	ASD – MSO Controlled Flexible Usage Rights	GSD Guarantees of QoS, Consistent UI	AOD	ASD+GSD	AOD+GSD	BED
Security	Authentication plus CA or in-home DRM based on NGNA NCSP	None	CL Approved Output Interface to ASD	Authentication & CA or in-home DRM	CL Approved Output Interface to ASD	None
QoS	Prioritized QoS (UPnP QoS) - **Optional**	Parameterized QoS (CableHome or UPnP)	None	Parameterized QoS (CableHome or UPnP)	Parameterized QoS (CableHome or UPnP)	None
Consistent UI	Desired	Yes	None	Yes	Yes	None
Management	CableHome PS** (for Gateway) or CableHome BP*** (for client) - **Optional**	CableHome PS (for Gateway) or CableHome BP (for client)	None	CableHome PS (for Gateway) or CableHome BP (for client)	CableHome PS (for Gateway) or CableHome BP (for client)	None
Discovery	UPnP/DLNA	UPnP /DLNA	None	UPnP /DLNA	UPnP /DLNA	None
Services	Protected, Non-QoS sensitive content Services with full flexibility to set usage rights	Unprotected, QoS sensitive content services e.g. Interactive game-playing, Voice, Video Phone.	Protected, non-QoS sensitive content services with limited flexibility to set usage rights	High-value content services with full flexibility to set usage rights	Protected, QoS sensitive content services with limited flexibility to set usage rights	Unprotected, non-QoS sensitive content

* This table assumes that all devices in these domains have a home networking interface.

** CableHome PS includes the functionality of UPnP Control Point.

*** CableHome BP is a superset of UPnP QoS and other UPnP functionality

If NGNA home network management is unavailable, NGNA-compliant CPE devices should continue to operate, although possibly at a reduced level. Programmable devices can be conforming when running certain applications, and non-conforming when running other applications.

The NGNA anticipates running compatible secure clients on the PCs so that rights-managed content can be exchanged between SVDs and PCs. An example of an application might be to watch on a PC video from a DVR housed in an SVD. Alternatively, a PC could take on the role of a video or music server allowing for SVD access to the PC content. For example, a PC could serve as an advanced home answering machine or caller ID information could be displayed on a TV.

2.5.2 Digital Rights Management

Content is delivered to each SVD within the Authorized Service Domain using the head-end managed CA. Each SVD includes peer-to-peer protocol support with copy protection provided by in-home networking digital rights management (DRM). The NGNA assumes that each device includes secure clients that can mutually authenticate to each other using digital signatures or a standardized key exchange technology. The NCSP can provide bridging capabilities between the cable network CA and the home network DRM.

In this NGNA in-home structure, an SVD on the network would have access to the features and content on any other device on either the GSD or ASD networks. By employing standardized algorithms for content encryption at the Rights Management System (RMS), the RMS is capable of supporting multiple video streams for recording, real-time viewing and multiple viewing sessions.

The NGNA RMS is capable of translating entitlements and copy protection states and transporting these rights throughout the in-home network. The NGNA RMS employs new concepts and technologies in the area of key management while functioning with existing legacy systems using key sharing or re-configuration criteria. Keys and Entitlements may be translated from the video stream Copy Control Information (CCI), ECMs, and EMMs to be loaded directly into the decryption engines without exposure in the content decryption engine on the home network device.

In the NGNA in-home rights management system, a Rights file that contains access criteria to various service tiers and a content decryption key typically would be signed and encrypted. The content key would be the key used to decrypt the content and may need to be changed on a variable periodicity. The entitlements and copy protection restrictions would be decrypted and checked in the CPE against the customer access criteria in order to provide authorization. If authorization were granted, the content key would be issued by the CA element and used to decrypt the content at the CPE device on the home network.

The NGNA RMS performs all key generation processing, encryption, decryption, digital signature processing and key exchange algorithms inside tamper resistant hardware/software, which is designed to completely prevent the modification or unauthorized disclosure/analysis of the processing, Critical Security Parameters, and private keys.

2.5.2.1 CA-DRM Linkage

The network CA is responsible for managing the NGNA RMS. All third-party DRMs should be approved as an acceptable output before the NGNA RMS will perform a hand-off of the content and rights. The DRMs are treated as part of the Approved Output Domain as defined above. To support any third-party DRM system not associated with the network CA, the NGNA RMS is used to translate rights into the third-party DRM. In addition, the NGNA RMS is used to authenticate any third-party DRM device before sharing content and rights information. The NCSP supports this hand-off process.

2.5.3 Use of Coax for In-Home Networking

Coaxial cable is an attractive physical layer for in-home networks. It is generally present in many rooms in the house and has ample bandwidth to support a myriad of bandwidth-hungry services.

An important issue in using the coax for in-home communications is ensuring that in-home network signals do not interfere with current or future services being offered through the coaxial cable from the cable company. In addition to frustrating the customer by preventing access to cable services, such interference could affect other cable subscribers on the same cable network segment/node.

For this reason, any in-home coax physical layer should respect and be compatible with the outside plant physical layer in terms of upstream and downstream spectrum, FCC Part 15 regulations, and with signal levels within the dynamic range of the plant; this can be accomplished via interaction with the head-end to ensure compatible use of spectrum (preferred) or through isolation of the home coax segment from the outside cable plant. In the latter instance, such isolation may interfere with delivery of future cable services and also generally requires installation of an isolating element, such as a filter, near the point of entry to the home, which can be inconvenient.

NGNA assumes that the in-home coax physical layer operating parameters are visible to and may be managed by head-end systems to ensure compatible use of spectrum. The reference architecture assumes that the head-end provisions the in-home physical layer with these operating parameters, e.g. upper and lower spectrum boundaries, and that once provisioned, the in-home coax physical layers operates within the limits defined by the head-end.

With regard to the in-home physical layer, the MAC layer should mediate traffic between devices on the in-home coax network. NGNA assumes that all devices on the in-home coax network are peer devices and that once these devices are provisioned by the head-end, they can share the in-home coax physical layer without any centralized management. The NGNA assumes a MAC layer protocol that operates in a peer-to-peer distributed fashion to prioritize traffic so as to maximize the user experience. For example, a protocol should be capable of assigning higher priority access to the media to streaming video traffic between devices on the in-home coax network than to delay-insensitive data traffic.

2.5.4 Content Sources and Clients

The in-home network architecture is specified to aid the seamless interoperability of content sources and clients. Content stores (i.e. music, photo and video libraries) that exist on networked clients may be discovered, cataloged, and streamed to other devices on the home network, and even optionally offered to authorized devices outside of the home network.

An objective for the in-home network architecture is to enable a convenient, unencumbered home network platform for the consumer while maintaining the integrity of protected (restricted) content within the Authorized Service Domain (ASD). Several assumptions are embedded within this framework:

- All content transport between devices connected to the in-home network is via IP (Internet Protocol);
- The network architecture will transport many different types of media, including video, audio, "stills" (e.g. JPEGs) and data;
- The network architecture will provide simultaneous support for MSO-supplied protected content and services, alternate-source protected content (e.g. a third-party music DRM solution), and non-protected content (regardless of source).

While there may be several in-home network architectures that achieve the desired goals, a number of key technical points should be considered:

- Only authorized (i.e. certified) devices may be part of the ASD.
- The architecture should support transmission and storage of both MSO delivered content and non-MSO delivered content.
- MSO-delivered protected content may be stored and consumed within the ASD.
- MSO-delivered protected content may only exit the ASD through approved outputs.
- Protected and non-MSO-delivered content may be consumed and stored within the ASD.
- Unprotected and non-MSO-delivered content may freely exit the ASD for consumption on a non-trusted device if the device follows the FCC's applicable Broadcast Flag rules.
- If the communications link with the cable network is disrupted, the in-home network architecture should still function for up to a certain length of time, with the time limit set by the cable operator.

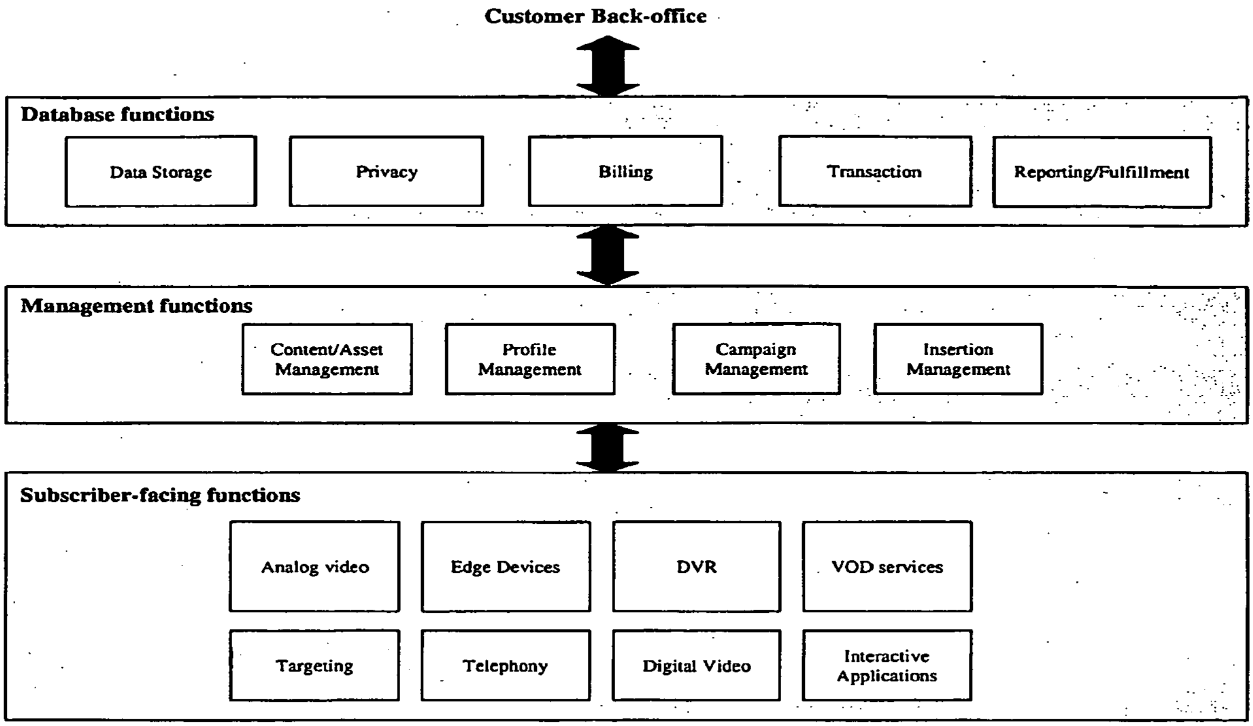
2.6 Advanced Digital Advertising

NGNA supports the transition of advertising on cable from analog to digital ad insertion, and it enables a wide variety of advanced advertising models such as:

- Digital-into-digital advertising
- Targeted and addressable advertising
- Interactive advertising (on all services)
- DVR advertising
  - Long form– content distributed and stored locally on the DVR
  - Replacement - refresh previous recorded ad content on the DVR
  - Network DVR - refresh previous recorded ad content on nDVR
- VOD advertising
  - VOD content advertising support - bumper or interstitial advertising content
  - Local VOD ad insertion - support for local ad insertion in ad-supported VOD content
  - VOD publishing for an advertiser
- Data collection across all advertising services to include synchronized content
- Insertion of national, regional, and local advertising at all points within cable physical plant as well as from sources outside the plant such as the Internet.

The functional breakdown of the advanced advertising architecture includes database, management, and subscriber facing functions, as shown in Figure 9 below.

Figure 9. Advanced advertising functional architecture



2.6.1 Database Functions

Collection of data and ability to access advertising related data is supported for the following purposes:

- **Data Storage** – Data related to ad-supported content is stored in raw form for analyzing/ monitoring function capability. These data, which will include advertising application data, profile data, viewership data and click stream data, should be collected in a standard/unified manner and should be definable on an MSO level with open business rule definitions. The data will be collected at:
  - *Viewer level* – viewership interactions on a time and content source basis; relationships between services and applications; timing of viewed material across content sources;
  - *Ad insertion level* – as advertising is inserted at an edge device or in a service or application;
  - *Advertiser customer level* – all information from content/asset manager; data collected at aggregate level from the profile manager;
  - *Management level* – operational data to support management functions.

- **Privacy** – Methods to protect the individual privacy of cable subscribers privacy build on current practices that include aggregating and anonymizing change of state data; and protecting the externally viewable data from being directly associated with a MAC address (for example, by transcoding of the MAC address to another identifier). Such techniques also facilitate the sending of targeted ads to very granular demographics while protecting the identities of the recipients. All privacy techniques allow for the individual MSO privacy policies that may include opt in/ out procedures and related business rules.

- **Billing** – The architecture enables collection of advertising client billing data with affidavit information to allow billing of the advertising customer in a single unified manner. These data will include information related to spot insertions, VOD advertising campaigns (VOD long form content and refreshing of VOD ad supported content), locally produced cable content, and interactive campaigns, e.g., fulfillment fees, interactive ad campaigns and telescoping.

- **Transactions** – The architecture supports subscriber requests for information and TV-commerce data collection, for example to enable automatic provisioning of a new service via an interactive advertising campaign. Such data may also need to be sent on to an advertising customer after an appropriate opt-in process.

  NGNA provides means to protect the privacy of subscriber transactional data on the return path including personal identifiable information such as individual names, social security numbers and credit card information.

- **Reporting** – Data for advertisers and for the operator will report on subscriber usage and analyses, fulfillment/transaction activities, click stream analysis, data affidavit (audit) capability, and will support AAAA (American Association of Advertising Agencies) collection needs.

2.6.2 Management Functions

Advanced digital advertising needs to be consistently managed for effective control of the advertising business, requiring *Content Asset Management*, *Profile Management*, *Campaign Management*, and *Insertion Management*.

Content Asset Management: This refers to ingest of content into the system and the movement, tracking and control of the content for both execution, contractual, and reporting needs. NGNA compliant systems should be capable of management in the following dimensions:

- Programming content management
- Commercial asset management, including traditional video and audio elements, or a variety of individually isolatable components - video, audio, data, graphic elements, XML/metadata, and iconography
- Metadata standards/requirements
- Ad standards (AAAA, ANA – Association of National Advertisers, CAB – Cable Advertising Bureau)
- Watermarking, to identify and confirm that spots have been telecast in the programs and at the times contracted; a digital watermark is inserted within the commercial asset to confirm telecast as contracted. This capability could be

transitioned to a non-linear environment to confirm delivery of a commercial asset to an individual or CPE device.

- Standard linear ad lengths plus non-linear commercial assets such as telescoped ads, bugs, overlays, and interactive advertising, e.g., polls, requests for information, and couponing.
- Digital Rights Management (DRM) to control altering of ad content.

Subscriber Profile Management: This refers to targeting of content based on assets, campaign details and subscriber profiles, with special attention to privacy issues.

Historically, broadcast advertising is a one-to-many messaging system, in which the relevance, appropriateness, and timeliness of a commercial asset's transmission is incompatible with a large segment of the viewers. The emerging advanced digital advertising methodology implies a one-to-one advertising capability more analogous to "direct mail" or "yellow pages" advertising: meaningfulness of the advertising to the recipient benefits both the sender and the receiver.

The identification, acquisition, warehousing, and mining of viewer profile information are important to the successful enhancement of traditional broadcast television techniques in the transition of these capabilities to advanced digital advertising. This information should be handled in accordance with all applicable privacy laws and business rules to ensure that the viewer's personal identifiable information (PII) is protected. Typically, the information derived will only be used in aggregate unless the subscriber has agreed to provide personal information through an "opt-in" process. Profile information may consist of implied data that are derived through analysis; frequently, these data are available through the use of third party databases and other publicly available information. These data indicate a household or viewer's traits defined, for example, by geographic location or demographic propensities. Subscriber profile information may also be derived through analysis of program selection and viewing, and through clickstream analysis concerning subscriber consumption of program content and commercial assets.

Profile analysis supports enhanced commercial asset delivery through:

- *Targeting* – delivery of an advertising message to a unique group of subscribers self-defined by the topography of the cable system. Although basically geographic in nature, hypotheses of demographic and psychographic information that are tied to geography can be extrapolated and utilized to enhance commercial asset delivery.

- *Addressability* – identifying individual households and/or CPE for delivery of commercial assets "addressed" to a particular consumer device, equivalent to "direct mail." Individual addressability may be achieved through correlation of program viewership and household CPE, although true one-to-one addressability implies viewer self-identification through the user interface with the CPE when the program viewing begins.

- *Interactivity* – includes a range of possibilities such as a subscriber picking a subject or advertiser of particular interest from an EPG screen and watching a long-form advertisement; or, a subscriber clicking on a screen logo during a standard advertisement and then being directed or automatically transitioned to a relevant long form advertisement or taken to a site or portal where information can be provided that enables a customized response or follow-up by the advertiser.

- *E-business* – subscriber purchase of an advertised item or interaction with the TV in response to a "product placement" during an entertainment program.

In the more extensive forms of interactivity, a user profile assists in expediting the purchase experience by ensuring availability of relevant name, credit card, address, and other information.

Campaign Management: This refers to business rules of the ad campaign, length of run, target criteria, etc., allowing the maximization of flexibility to advertisers without artificial constraints encountered in traditional linear analog systems. This entire process includes multiple steps including research, planning, proposal, contract/traffic, continuity, execution, verification, and billing. Each of these steps may include multiple iteration loops within and spanning the various processes. Open APIs are needed to allow various systemic components to be individually selected, including research, planning, proposals, contract/traffic, copy (continuity), execution, verification, and billing.

Insertion Management: This refers to decision-based transport and especially takes into account linear, non-linear, and the variety of digital presentation standards that will be encountered. The management functions culminate in the actual insertion of the commercial asset into the proper program content to be seen by the appropriately profiled viewer as determined by the advertiser campaign. This is true whether dealing with a linear or a non-linear environment.

NGNA supports (or at least does not impede) an operator's ability to utilize or create an avail. Opportunities for avails happen at multiple locations during the delivery to the consumer. A few of the methods of utilizing avails are:

- Splicing content into analog or digital broadcasts;
- Creating playlists of content stored on a video server or DVR;
- Inserting ad content during the production of a video;
- Inserting cue point in a stored video that triggers an insertion to happen.

Content may be spliced or inserted on the delivery chain in such current and future locations as:

- Analog or digital broadcast at the head-end;
- Digital broadcast at the hub/node (this can be accomplished at the head-end with transport mechanisms);
- Playlist creation on a VOD server;
- SVD splicing between input streams;
- SVD DVR (playlists, switching, splicing).

NGNA enhances and facilitates advertising insertion opportunities. Areas to be considered include:

- **Codecs** – NGNA-compliant CPE enables non-obvious, visual and audio seamless transitions between program content and commercial assets regardless of the codecs and/or screen resolutions associated with each.

- **Encryption / Decryption** – Since the insertion of commercial assets into program content is anticipated at a variety of locations throughout the network, care should be taken to consider the implications of encryption on the program stream. Since splicing should occur in an unencrypted stream, design considerations are preferred that will minimize the need to encrypt/decrypt repeatedly.

- **Commercial Asset Encoding** - In order to insure that the *ad hoc* splicing of commercial assets into one or more multiplexed streams occurs without disruption to the spliced stream or to other streams within the multiplex, the commercial content should be encoded at a data rate that as closely as possible matches that of the program content. In addition to visual quality, special attention should be paid to audio encoding. Unlike the analog environment, the matching of audio levels between program content and commercial assets cannot be achieved through the use of traditional "gain controls." Tightly coupled techniques are necessary to ensure that levels are matched.

- **Transcoding – Formatic Display** – In digitally splicing commercial assets into program content, the preferred result is that the splice will have occurred in a visually seamless manner; although both video sources may have been encoded at various bit rates and with different resolutions and formatic displays, any transitions should be visually unapparent. It is preferable for a commercial asset to be encoded a single time; ideally the encoded file is transformed on the fly to match the "format" of the program stream into which it is spliced. Alternately, if multiple copies of the commercial asset are to be maintained for (for example an "SD" version and an "HD" version), the systems associated with the traffic, copy and insertion functions should minimize the need for manual provisioning, tracking and reporting of multiple "copy numbers".

2.6.3 Subscriber-Facing Functions

Subscriber-facing functions are functions that the subscriber will see or interact with:

- *Analog Video* – traditional analog ad video insertion, graphical overlays of existing commercial content, ad triggers to set up on-demand session; adding functionality to local spot sales through "hyper-targeting", copy split, increased tagging capabilities.
- *Digital Video* – digital video insertion, multi codec support; supporting local ad sales insertion; hyper targeting of ads based on SVD usage and outside data additions.
- *VOD Services* – long form advertising-on-demand (LFA), currently defined as anything longer than 2 minutes; enabling HTML session off of on-demand servers; trigger for more information from advertisers in on-demand programming; e-commerce solutions to facilitate actual transactions.
- *DVR /nDVR* – LFA on disk; SVD based interactions; Network DVR triggering device.
- *Interactive Applications* – interactive television, web on TV, IPG/EPG; polling; RFI (Request for Information); e-commerce.

- *Telephony* – sponsored caller ID; ad-supported Voice Mail.
- *Edge Devices* – stream switching ads at the node.
- *Iconography* - key icons or remote control buttons that will be reserved for interactive TV.

These subscriber-facing functions should have similar advertising related CPE features and consistent open APIs to support the widest range of advertising based services.

2.6.3.1 CPE Requirements

A ubiquitous applications environment is important to enable cost effective deployment of interactive ads and ad based services. OCAP provides a robust environment for most functions. A lightweight XML-based environment is also in development to support simple interactive applications for OCAP and non-OCAP CPE. This format may be useful for simple interactive ads. Certain network signaling is also necessary to support some CPE applications.

2.6.3.2 APIs

The following APIs are needed to support a wide range of advertising based services:

- **DVR** – OCAP currently supports DVR functionality. These APIs allow pre-loading of spot ads and LFA, and seamless switching of streams and content management on the DVR device.

- **VOD** – OCAP currently does not include a session management API, because different VOD vendors support different session protocols. A mechanism exists to install a network specific API, but this does not allow an application to be interoperable between networks.

- **Data collection/profiling** – OCAP provides applications with the ability to store and report user events, however, there may be several applications running at one time, and there is no way to collect a comprehensive 'click-stream' at the application level. An API that enables system level collection, compression, encryption, and reporting is desirable. Such an API allows users to 'opt-in' to data collection, and gives applications fine-grained control of all aspects of data collection.

2.6.3.3 Network signaling

Advanced advertising applications are supported by a variety of network signaling mechanisms, including boundary markers, cues, and triggers.

- **Boundary markers** - In order to switch or splice ads into other programs, the ad avail boundaries should be visible to splicing applications. These boundary markers are embedded in a digital transport stream and are used for in-network splicing (see SCTE DVS 35). The NGNA CPE may be a retail product, and therefore CE manufacturers are expected to ship devices with their own set of applications. To protect advertiser-supported services, these markers could be stripped from the digital stream and delivered to trusted applications over a secure channel.

- **Cues** - Cues refer to data packets embedded in a program at regular intervals to provide timing information to an application. DSMCC stream events may be used for digital services, and VBI data may be used for analog. Cues create a 'click-track' that applications may use to synchronize with video programming.
- **Triggers** - Triggers provide a means for synchronizing an application with a program. Triggers may be encoded in VBI for analog programs, in a DSMCC stream event for a digital service, or may be delivered via an alternate channel as a playlist. Triggers may employ one of three temporal models:
    - Absolute time: indicates that the application should do something at a specific time and date;
    - Relative time: Indicates that the application should do something at an offset from the beginning of the associated program, e.g., display text 12 seconds into a spot;
    - 'Do-it-now': Indicates that the application should react as soon as it detects the signal.

2.6.3.4 Interactive advertisements

OCAP will provide a nationwide footprint for deployment of interactive advertisements. These applications may be embedded in a digital transport stream or deployed by the network operator via some other channel. The OCAP Java environment is full featured and, except for certain items identified above, provides the means for advertisers, programmers, and network operators to deploy a wide range of applications.

3.0 Customer Premises

This section describes the essential elements of NGNA-compliant video and non-video CPE devices, with the intent that the platform is as unconstrained as possible.

3.1 Overview

The customer premises network segment involves significant opportunities and challenges vis-à-vis consumer electronics manufacturers, CE retailers, and FCC regulations, as well as representing the largest overall investment given the large number of devices. CPE will vary in their capabilities. For example, options include support for gateway services in the home data network, and digital video recording (DVR). The following table summarizes key features and attributes of a range of NGNA compliant CPE devices.

Table 3. CPE Feature Overview

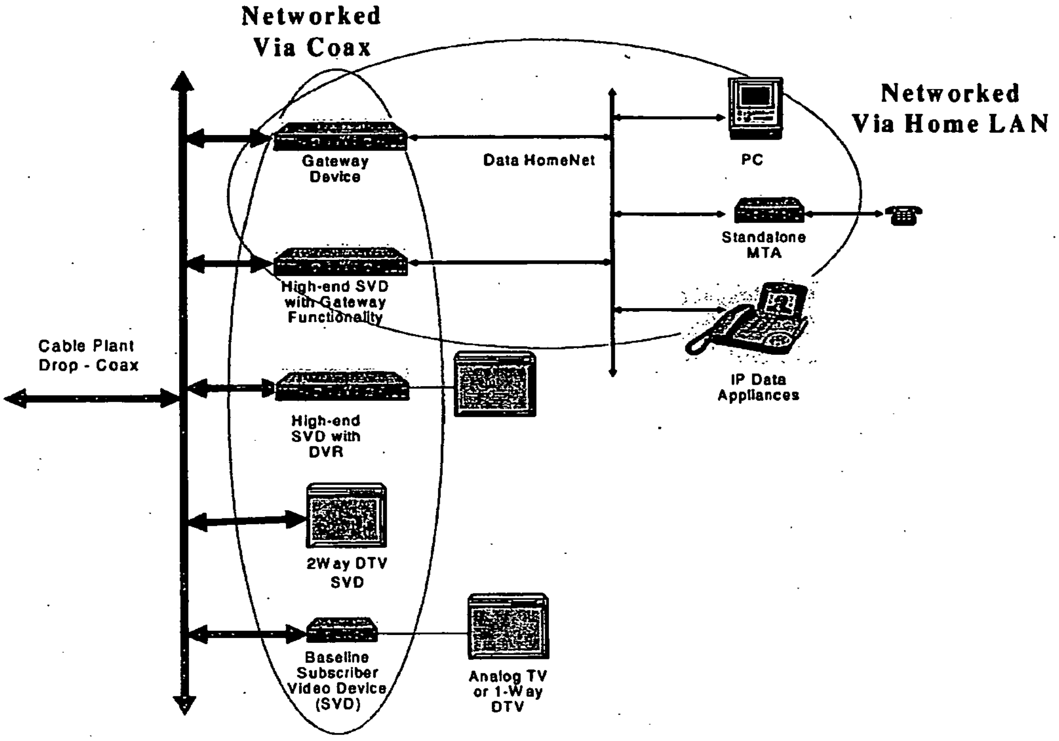
	Baseline SVD	Extended SVD (Non-Gateway)	Extended SVD (Gateway)	Media Client	Video NIU
NCSP Support	✓	✓	✓	✓	✓
DOCSIS 2.0	✓	✓	✓		✓
Tuner support	✓	✓	✓		✓
Extended SVD functions other than Gateway (e.g., DVR, CableCard, display)		✓	✓	TBD	
Home Network Gateway (CableHome Portal Services, UPnP Control Point)			✓		
Home Network Client (CableHome Boundary point, UPnP signaling, UPnP QoS)	✓	✓		✓	
OCAP capable	✓	✓	✓	Optional	
USB 2.0 host	✓	✓	✓	✓	

3.2 Subscriber Video Devices (SVDs)

Subscriber video devices (SVDs) include devices with a minimal core of NGNA-compliant capabilities, up to devices that provide a richer set of capabilities. This equipment will be provided either by the cable operator or at retail by consumer electronics suppliers. SVDs will operate as set-top or set-back boxes. Other SVDs could include two-way cable-ready digital TV sets.

These devices are designated as SVDs because each provides more than the conventional set-top box functions, such as re-configurable CA via an NCSP, support for an advanced video codec, support for multiple video transport options, and for networking over the in-home network. Each SVD can access resources in or provide resources to other devices on the network. In other words, all SVDs may act as source or destination of content within the in-home network. Thus through the in-home network the lowest order device can deliver some of the features and capabilities of the highest order device. The NGNA provides for copy-protected and rights-managed interchange of content between any of the SVDs on the home network. Figure 10 illustrates the SVDs' ability to network to other SVDs and to other compatible devices.

Figure 10. Example of SVD deployment for subscriber with home data network.



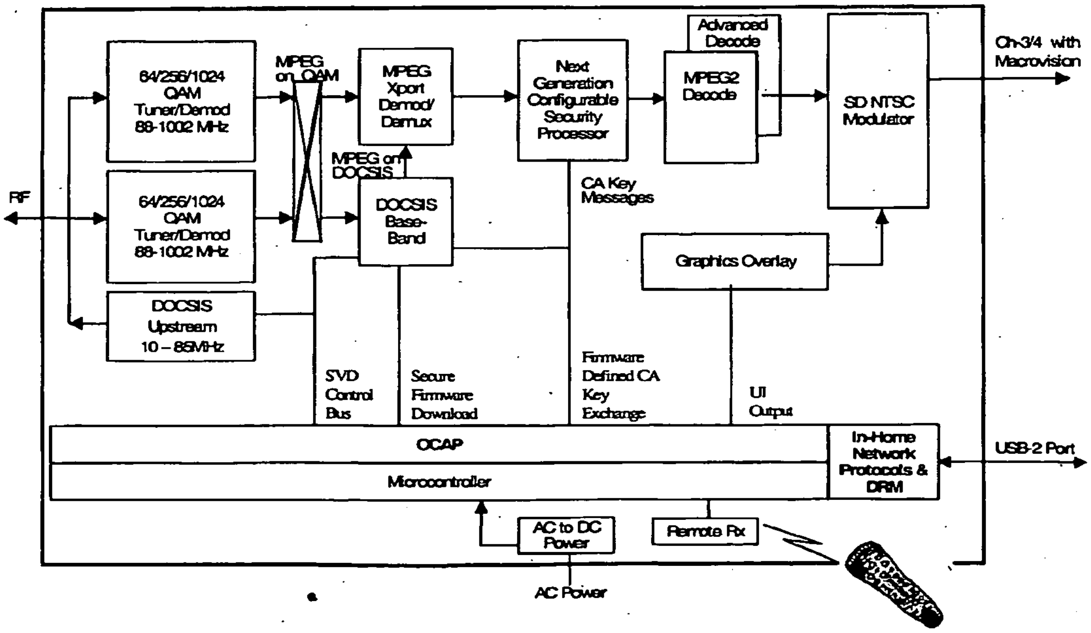
SVDs have as their principle function the delivery of video entertainment. Additional devices may offer video communications and may be networked with SVDs, such as video conferencing devices and other forms of IP appliances. The baseline SVD includes the following functionality:

- All digital, standard definition video decode (MPEG-2 and advanced codec).
- Standalone device (does not function as a TV).
- Supports both 1-way and 2-way services.
- OCAP capable - the intent is to have SVDs run OCAP middleware.
- Compatible with the NGNA security architecture, as described earlier, with internal NCSP.
- Two tuners. Either tuner should be capable of supporting any of the three NGNA-defined transport mechanisms. For example, one tuner could support DOCSIS 2.0, while the other tuner would support MPEG-2 transport over QAM.
- Support for DOCSIS 2.0 as modified with an expanded frequency range consistent with future mid-split migration.
- Downstream tuning range is 88-1002 MHz. The lower downstream tuning frequency is bounded at 88 MHz to support future mid-split plant designs.
- Upstream transmission range is 10-85MHz.
- Video may be delivered as either MPEG transport packets over QAM, or alternatively over the DOCSIS 2.0 path. In addition, video may be delivered over in-home network, encapsulated in IP, as described earlier.

- Supports MPEG-2 as well as the advanced video codecs described earlier.
- Supports Dolby AC-3 (stereo) audio.
- Basic support for in-home networking is provided by the presence of a USB 2.0 port. Various networking "dongles" can be attached to this port to provide PHY/MAC layer functionality for different in-home networking architectures (e.g., Ethernet, WiFi, MoCA).
- The baseline SVD is a Guaranteed and Authorized Service Domain device, as defined earlier.
- The device functions as an in-home network client, which requires the device to function as CableHome Boundary point and to provide UPnP signaling and UPnP QoS.
- The device also supports an expansion port that allows hardware renewability of the internal security mechanism.
- Video output is provided by a single RF composite video port or approved digital video interface.
- A companion universal remote control is provided that can be additionally configured by the subscriber to operate an existing TV and/or VCR. The remote should support IR technology at a minimum, with RF support being optional. In addition, the remote should be compliant with the OCAP requirements for remote control devices.

Baseline SVDs may assist in the transition to all-digital services. Used for this purpose, baseline SVDs will allow subscribers who have cable-ready analog TVs and other analog devices (e.g., VCRs) to continue to receive their existing services in a manner that is as transparent as possible even though the formerly analog channels will have been re-assigned to carry digitally compressed signals. Baseline SVD functions are illustrated in Figure 11 below.

Figure 11. Baseline SVD functions

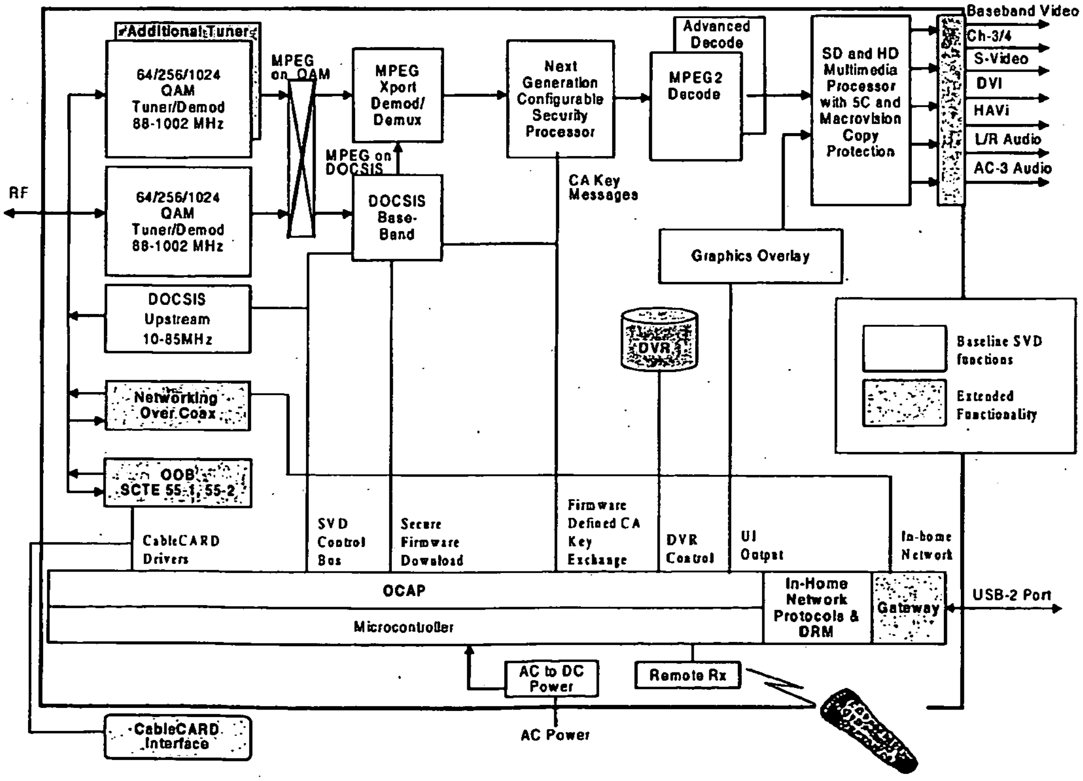


SVD suppliers may provide additional extended functions in higher-end devices. For example, these features may support:

- High definition video signals, including the following authorized digital outputs: DVI (or HDMI) with HDCP and 1394 with DTCP.
- Multi-tuner support for receiving and processing multiple video programs.
- DVR functionality, including both internal and external storage.
- CableHome Gateway functionality, which requires the device to support CableHome Portal Services and function as a UPnP Control Point. In addition, devices that support Gateway functionality should support the ability to enable and disable this feature to avoid conflicts if multiple gateways are installed on the same network.
- CableCARD support.
- On-board support for networking connectivity (e.g., MoCA, WiFi, HomePlug). This support is in addition to the required baseline USB-2 port and associated network "dongle" support.
- Associated display such that SVD functions as two-way DTV.

While NGNA does not require NTSC analog tuner support, an SVD that does include this feature would have to comply with applicable FCC rules concerning DTV devices that incorporate NTSC. Figure 12 shows capabilities of a baseline NGNA SVD plus extended features that may be found in higher-end SVDs.

Figure 12. Baseline SVD Architecture and Possible Extended SVD Functions



All SVDs are required to meet appropriate content protection compliance and other rules to ensure that services delivered in the Guaranteed and Authorized Service Domains are delivered as intended by the cable operator.

3.3 Other CPE Devices

The NGNA describes examples of next generation network CPE in addition to options for SVDs.

3.3.1 Video Media Client

The video media client is a "tuner-less" device that is designed specifically to connect to other SVDs on the in-home network in order to receive video content. It may provide a rich application environment through on-board middleware and applications, or may instead present a "remote user interface" that is driven by the SVD serving it content.

Some of the baseline features for the media client include:

- Standard definition, digital only
- In-home DRM support as provided by NCSP
- In-home networking client support
- Device may function as an ASD device or as a GSD/ASD device
- MPEG-2 and advanced codec support
- Companion universal remote control or controlled via remote that communicates with source device
- USB 2.0 for providing network connectivity

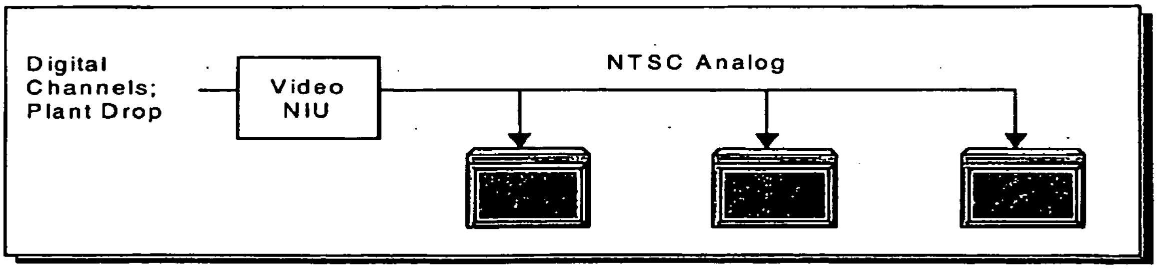
Optional features of the media client include:

- High definition support with associated approved digital outputs

3.3.2 Video Network Interface Unit (Video NIU)

In some subscriber households with numerous analog cable outlets, it may be economical to provide analog functionality to the home through a digital-to-analog block converter at the service entrance. This device would provide whole-house coverage rather than requiring SVDs at each analog device.

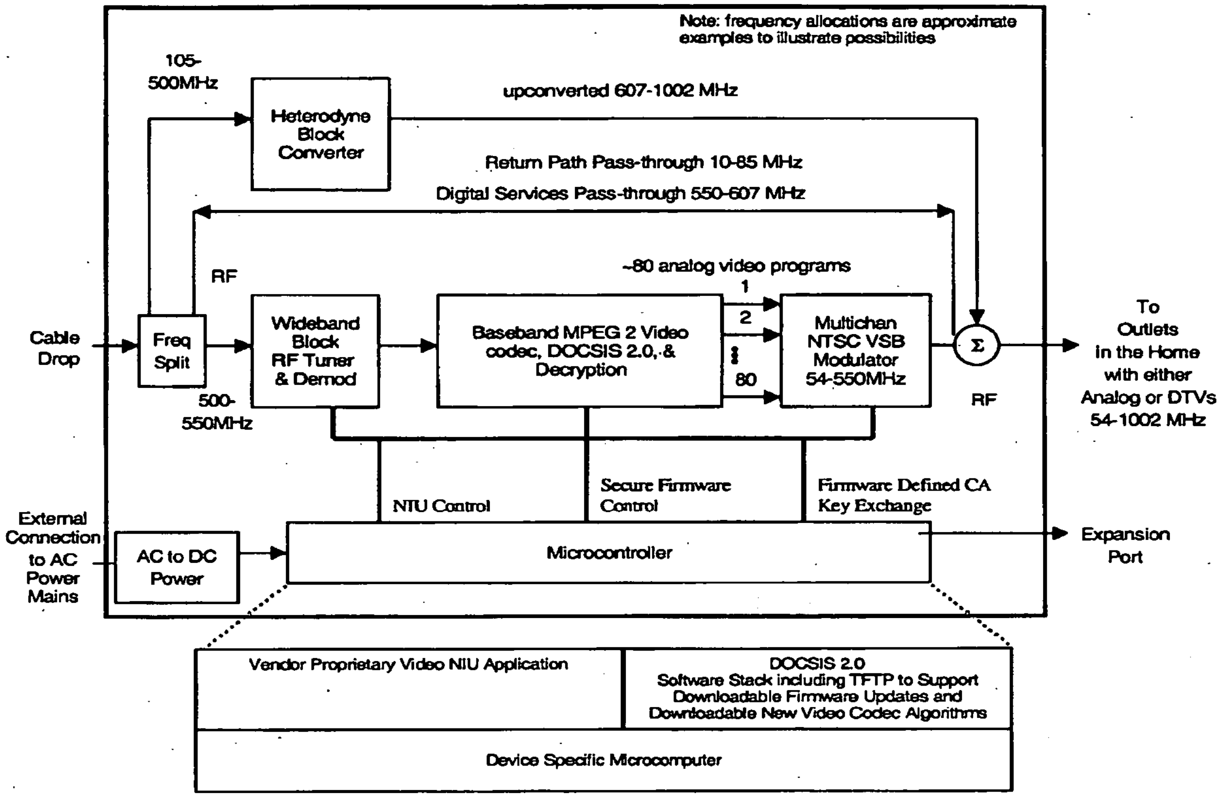
Figure 13. Example of Video NIU deployment



The Video NIU is intended as a device that allows subscribers who have cable-ready analog TVs and other analog devices (e.g. VCRs) to continue to receive their existing services in a manner that is as transparent as possible, while the formerly analog channels are used to carry digitally compressed signals on the cable plant.

The Video NIU performs a block transcoding of digital signals on the plant to analog signals within the home. The following diagram shows a possible NIU architecture.

Figure 14. Video NIU Hardware Architecture


Note: frequency allocations are approximate examples to illustrate possibilities
105-500MHz
Heterodyne Block Converter
upconverted 607-1002 MHz
Return Path Pass-through 10-85 MHz
Digital Services Pass-through 550-607 MHz
RF
~80 analog video programs
1
2
80
Cable Drop
Freq Split
Wideband Block RF Tuner & Demod
Baseband MPEG 2 Video codec, DOCSIS 2.0, & Decryption
Multichan NTSC VSB Modulator 54-550MHz
Σ
RF
To Outlets in the Home with either Analog or DTVs 54-1002 MHz
500-550MHz
NIU Control
Secure Firmware Control
Firmware Defined CA Key Exchange
External Connection to AC Power Mains
AC to DC Power
Microcontroller
Expansion Port
Vendor Proprietary Video NIU Application
DOCSIS 2.0 Software Stack including TFTP to Support Downloadable Firmware Updates and Downloadable New Video Codec Algorithms
Device Specific Microcomputer

Baseline features of Video NIU include:

- Allows for migration of some (or all) analog channels on the plant to compressed digital.
- Provides greater transparency to existing subscribers with no set-top boxes as there is no need to use a special remote control and there would be no latency in channel surfing.
- Compatible with future mid-split designs.
- Compatible with NCSP and DOCSIS signaling used in the NGNA architecture.
- Intended as a service-entry device that receives a wideband RF signal with compressed MPEG programming. In turn, these programs are decrypted, decompressed and NTSC encoded onto the in-home coax network.

- Does not prevent the carriage of other digital signals (including two-way services) on the in-home coax network. In other words, other CPE equipment would not be adversely affected by the presence of an NIU.
- Able to support both in-home and side-of-home deployment scenarios.

Key points to be addressed with NIU designs include:

- Deployment scenarios, including in-home and side-of-home.
- Powering of the device given the deployment scenario.
- Number of channels to be block decoded.
- Possible "switching" models where fewer numbers of channels are decoded simultaneously.
- Constraints on encoding of formerly analog signals.
- Constraints on in-home coax frequency spectrum, including the placement of non-analog services.

3.3.3 Non-video CPE

Given the proliferation of new video, data, and multimedia services, and increasing convergence between these services, it is likely that additional next generation non-video CPE will be developed that will connect directly and indirectly to the cable network.

Device manufacturers are already incorporating multiple functions into cable modems such as various combinations of layer 3 router firewalls, data hubs, voice telephony MTAs, and home networking transport (e.g. WiFi, HPNA, HomePlug, etc), and are likely also to integrate some of the next generation network functions into future cable modems and other subscriber devices. Next generation network functions that are candidates for creative integration into CPE include in-home networking within and between the guaranteed and authorized service domains, and CableHome functions that allow management and visibility of subscriber devices from the head-end.

Non-video CPE example: Multifunction gateway. The core of this device is currently available, including a cable modem, layer 3 router firewall, and a voice telephony MTA. A next generation version of this device would add CableHome capabilities of visibility and remote management from the head-end. It would also include a bridging feature allowing interaction between SVDs compatible with the in-home network protocols and CPE on the in-home data network. Such a device would support applications such as:

- Allowing PCs with a suitable bridge to use the coax network as a means to access high-speed data services.
- Allowing consumer-owned PCs or servers on the in-home data or coax network to communicate displayable messages or control messages to SVDs.
- Enabling the telephony MTA to send caller ID messages (or other messages) to SVDs.
- Allowing SVDs to access billing or service information regarding subscribers' interactive multimedia/data services.

4.0 Outside Plant

Cable operators are rapidly adding new services and capabilities while migrating from largely analog to digitally-coded downstream signals. Substantial growth in bandwidth-intensive HD programs is anticipated. Various forms of on-demand services are being introduced and, depending on how they are implemented, they could result in either more or less consumption of downstream bandwidth resources. In the upstream direction, applications are emerging such as voice telephony, telecommuting, peer-to-peer file exchange, and multiplayer gaming that will require more symmetrical upstream bandwidth allocations.

While accommodating the new applications, the outside plant needs to continue to support legacy investments in subscriber and head-end equipment. For example, the need to support legacy digital set-top boxes with proprietary CA during the time period while MSOs may choose to transition to a new proprietary or non-proprietary CA suggests a potential need to partly simulcast program content in both legacy as well as the new CA.

By employing advanced technology at the head-end and, in subscriber premises, NGNA can provide increased downstream capacity using the recently rebuilt capabilities of most cable outside plant to 750MHz bandwidth and 500 homes passed per fiber node.

4.1 Migration to Mid-split

NGNA supports future needs for increased upstream bandwidth by providing an evolutionary migration path from today's low split systems to future mid split systems. This migration path is enabled through a new spectral map for NGNA systems:

- *Upstream access plant*: Migration to 10MHz - 85MHz from 5MHz - 42MHz. 10MHz was designated as low limit to avoid the generally unused 5-10MHz spectrum that negatively effects upstream laser capacity due to ingress from impulse noise sources. 85MHz was selected as upper limit to stay below the 88MHz start of the FM broadcast radio band. The 3MHz guard-band between 85MHz and 88MHz is provided so that a filter can be implemented to minimize potential ingress from high power FM broadcast radio operations.

- *Downstream access plant*: Migration to 105MHz from 54MHz low limit. 105MHz was selected to maximize the forward passband with available crossover filter technology. Selection of 105MHz offers the ability to transmit certain legacy carriers between 105 and 108MHz.

Based on these spectral map choices for the outside plant, NGNA CPE are defined as capable of downstream tuning between 88MHz to 1002MHz. The mid-split migration plan calls for the full range down to 88MHz to be used prior to migration to mid-split. Once the migration to mid-split is completed, NGNA subscriber devices will not need to tune below 105MHz.

Setting the limit at 88MHz versus 54MHz will simplify the design of NGNA subscriber equipment RF front ends by not requiring the wide dynamic range rejection of high power upstream carriers between 54MHz to 85MHz once mid-split upstream is activated. Also, the band between 54MHz and 88MHz is likely to carry analog channels until the mid-split transition and NGNA compliant subscriber video devices are only required to support digital video signals.

Migrating to mid-split could be expected to yield results approximately as shown in the following table, with upstream throughput on the order of 345Mbps.

Table 4. Approximate upstream throughput with mid-split plant architecture

Typical Modulation Type	Efficiency, bits/Hz	Suitable regions, MHz	Total Bandwidth	Throughput, Mbps	Dominant Impairment
QPSK	1.6	10-20	10 MHz	16.0	Impulse
QAM16	3.2	20-26	6 MHz	19.2	Narrowband
Citizens Band	N/A	26-27	1 MHz	0	CB
QAM256, ATDM	6.4	27-44.5	17.5 MHz	112	Thermal
QPSK reduced level	1.6	44.5-50.5	6 MHz	9.6	TV IF avoid.
QAM256, ATDM	6.4	50.5-77	26.5 MHz	169.6	Thermal
QAM16	3.2	77-81	4 MHz	12.8	Delay
QPSK	1.6	81-85	4 MHz	6.4	Delay
Totals	0.8	10-85	75 MHz	345.6	

4.2 Status monitoring
This NGNA for outside plant adopts and incorporates by reference the SCTE HMS (Hybrid Management Sub-Layer Engineering Subcommittee) plans for status monitoring.

4.3 Other outside plant development
1GHz top frequency. Rebuilding to 1GHz is not required to meet NGNA objectives. However, it is notable that as a result of the outside plant rebuilds recently completed by cable MSOs, substantial portions of the hardware platforms installed are capable of passing a minimum top frequency of 1GHz. While not required for currently foreseen services that will be supported by the NGNA, it is anticipated that active upgrade electronics will continue to be developed that support graceful enhancement of downstream plant to 1GHz.

Digital upstream optical systems. It is anticipated that systems technology will be developed that supports processing of upstream digital signals at the optical transition node to enable upstream lasers to carry digital versus today's analog signals, thereby replacing analog with digital upstream optical systems.

Advanced modulation. It will be desirable for advanced modulation and error protection coding to be explored.

5.0 Head-end

Consistent with the vision of NGNA as an integrated multimedia architecture, NGNA head-end integration represents a significant departure from cable systems' traditional independent head-end "stovepipes" for video, data, and telephony. Benefits of integration include:

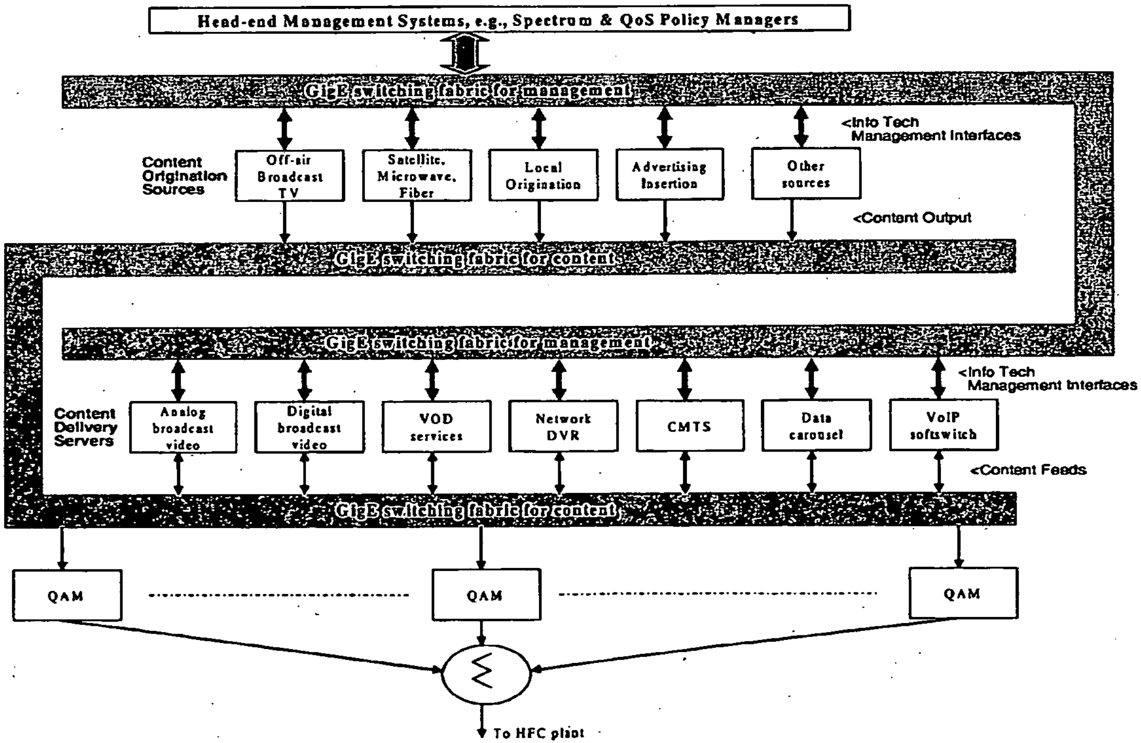
- More efficient use of system resources (e.g. spectrum allocations, QAM streams);
- Facilitate inter-working of network elements supplied by multiple vendors to enable more open competition, to extend the service life of the installed base, to provide flexibility for new service introductions, and to provide scalability to accommodate a range of system sizes;
- Provide a platform for innovation and rapid service creation that involves cross-over access among the former service stovepipes (e.g., viewing movies on a PC or caller ID on a TV).

This section describes the NGNA for the head-end, for head-end interfaces with the back-office, and for functions and capabilities that tend to be centered at the head-end, i.e., applications performance management.

5.1 Head-end network architecture

This section relates to the evolution of DOCSIS CMTS and QAM modulators, as well as sessions and resource management architecture. Figure 15 describes the overall head-end network delivery architecture.

Figure 15. Head-end network architecture


Head-end Management Systems, e.g., Spectrum & QoS Policy Managers
GigE switching fabric for management
<Info Tech Management Interfaces
Content Origination Sources
Off-air Broadcast TV
Satellite, Microwave, Fiber
Local Origination
Advertising Insertion
Other sources
<Content Output
GigE switching fabric for content
GigE switching fabric for management
<Info Tech Management Interfaces
Content Delivery Servers
Analog broadcast video
Digital broadcast video
VOD services
Network DVR
CMTS
Data carousel
VoIP softswitch
<Content Feeds
GigE switching fabric for content
QAM
QAM
QAM
To HFC plant

Key next generation features of head-end network architecture include:

- The head-end network enables the delivery of digital video traffic (encoded as MPEG transport streams) and generic IP datagram traffic (encapsulated in DOCSIS frames) over a common head-end network infrastructure.
- Applications are managed across all services by session and resource management systems, which should have capability to operate autonomously in the event of communications failure with back office systems.
- The control and RF aspects of the head-end servers are separate so that common third party resource management and network operations applications can manage the head-end as an integrated system rather than as standalone service specific subsystems.
  - *QAM modulators*: QAM modulators are separate from head-end servers such as VOD servers and the CMTS DOCSIS MAC, and each CMTS and Edge QAM is equipped with a GigE compatible data interface. Next generation, multi-channel, shared-upconverter edge QAMs will operate in the NGNA environment without causing impairment or degradation to the physical plant beyond what would be seen by adding that same number of simple single unit QAM modulators. Modified DOCSIS specifications will codify the edge QAM RF output parameters necessary to maintain the integrity of the RF plant.
  - *GigE switching fabric for content*: The GigE switch fabric will be under the control of a network resource manager for content distribution and will ensure that any server can have data switched to any QAM stream and that any content source can switch easily between content servers.
  - *Session and Resource Management system*: Application managers, session managers and resource managers will have functionality that gives the operator the ability to control and monitor traffic loads, QoS needs, and subscriber entitlements, and will have policies and algorithms to dynamically assign spectrum and QAM stream resources in the most efficient matter.
  - *Ethernet or GigE switching fabric for management*: The switching fabric will provide a standard management plane interface by means of an Ethernet or GigE switching fabric so that each service can be managed and controlled by external IT management systems via open APIs.
- IP, DOCSIS, and DSG (DOCSIS Set-top Gateway, for downstream-only communication) are used for the network transport of control and management messages to CPE. The set of signaling protocols for video-based services is likely to include DSM-CC (Digital Storage Media – Command and Control), RTSP, SIP, NCS/MGCP, and potentially XML-based "web services" protocols such as SOAP.

The following sections provide additional details on the separation of QAM modulators from the DOCSIS CMTS, and on the architecture for session and resource management.

5.1.1 Evolution of the DOCSIS CMTS and QAM modulators

Figure 16. Next Generation Head-End Network Architecture

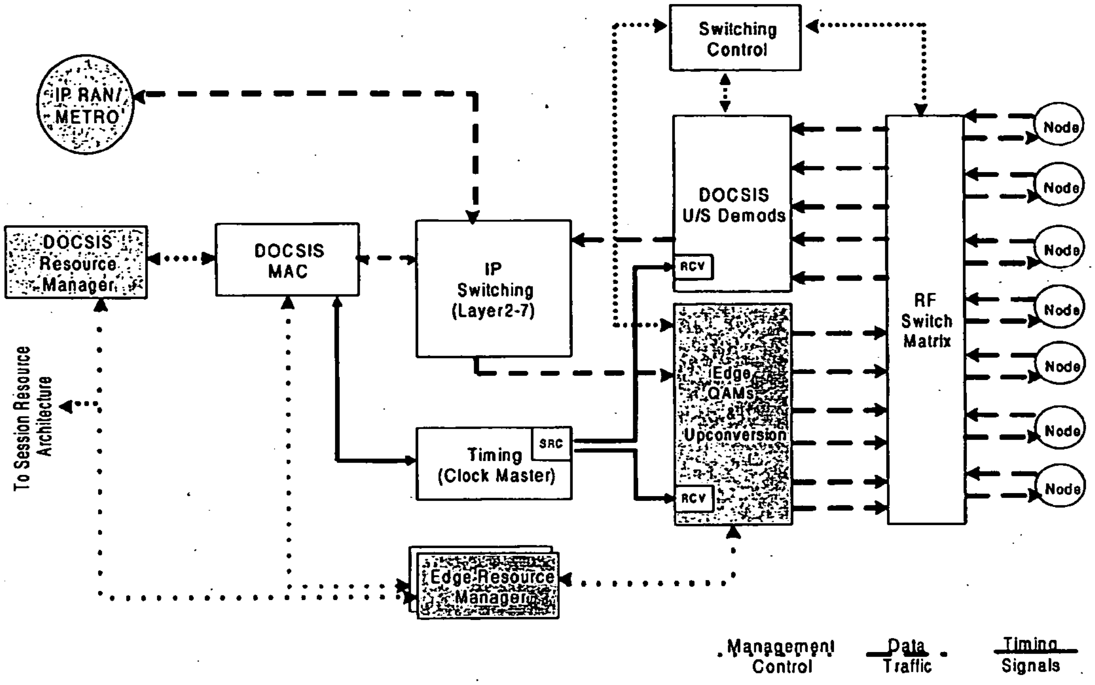


Figure 16 shows the functional components and their linkages. Several components in Figure 16 are considered as optional, including the RF switch and external timing interface. Components identified in Figure 16 are described below.

- **Edge Resource Manager**

The purpose of the ERM is to manage the allocation of Edge QAM resources for multiple applications such as VoD, DOCSIS, digital broadcast, etc. It is not intended to be inclusive of the inherent MAC processing that currently resides in today's CMTS.

- **DOCSIS Upstream (U/S) termination/demods (CMTS)**

In today's architecture, the purpose of the CMTS is to be the inclusive DOCSIS processing and Data distribution platform. Under NGNA, and to ensure the goal of facilitating the development of enhanced delivery systems, the CMTS will undergo several changes. One of the primary changes is separating the PHY (modulator and demodulator) and the DOCSIS MAC into separate devices. The MAC and PHYs in the NGNA architecture are connected via a low latency non-blocking switching network. The remaining CMTS functionality, such as scheduling, is included in the "DOCSIS MAC" component in the NGHE architecture.

- **DOCSIS MAC**

As depicted in the logical reference diagram, the DOCSIS MAC functions will remain the same. Features such as BPI+ processing, Packet Header Suppression, MAP Generation, and other DOCSIS centric features will happen at the central MAC. However, physical location of this functionality can vary based on scalability needs and other implementation scenarios.

- **Edge QAM**

Current Edge QAM devices handle both narrowcast and broadcast services received as MPEG-2 frames (carried over UDP). The Edge QAM depicted in the NGNA architecture will additionally need to receive downstream DOCSIS frames (carried in MPEG-2 transport over UDP). Provided to the Edge QAM is an external timing interface that supports the sync time stamps needed in order to meet low latency and jitter requirements currently listed in the DOCSIS specifications.

- **IP Switching (Layer 2-7)**

While not representing a drastic HW/SW departure, existing platforms can be levered with minor extensions to support low latency timing requirements. This component should be able to handle hundreds of gigabits worth of traffic, have distributed processing, flexible physical interfaces, as well as robust L3 features.

- **Timing**

The timing block function is to distribute a common timing source to the Edge QAM, DOCSIS MAC, and DOCSIS US termination blocks. A common timing reference may be needed to meet the DOCSIS jitter requirements. As depicted in Figure 16, the upstream (U/S) and downstream (D/S) timing source should be coherent in order to support both A-TDMA and S-CDMA that are required within the existing DOCSIS 2.0 specification. Although jitter and latency requirements are less stringent in A-TDMA, the requirement for both A-TDMA and S-CDMA capable systems will remain a component of the NGNA architecture.

- **RF Switch Matrix and Control**

The purpose of the switch matrix is to provide an N x 1 fault tolerant capability and cable once functionality. The switch control functions in concert with the PHY blocks work to deliver a "hitless" failover in the event of an Edge QAM or DOCSIS US failure. The switch matrix also allows all RF cabling from the plant to terminate at a common point that does not require re-cabling if any component in the Edge QAM or DOCSIS US needs replacement. The RF switch matrix is optional in deployments.

Although the diagram depicts the RF switch as a means to increase availability, alternative means to achieve high availability are acceptable.

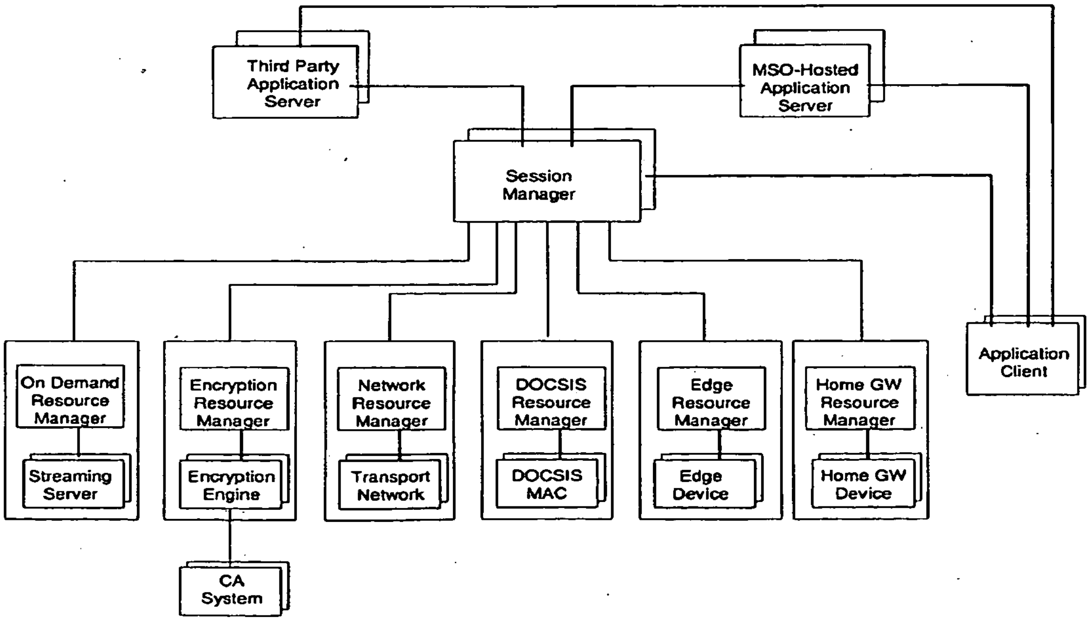
- **Wideband DOCSIS**
  The near-term need to increase bandwidth, especially on the downstream, can be achieved via the implementation of Wideband DOCSIS. This feature, where multiple 6MHz channels are bonded, can significantly increase throughput over existing DOCSIS specifications. A Wideband DOCSIS implementation will be backward compatible to existing DOCSIS 1.x and DOCSIS 2.x specifications. The primary component impacted by a Wideband DOCSIS implementation (with a downstream implementation) is the DOCSIS MAC.

DOCSIS specifications need to be updated to reflect the fact that high-density edge QAMs are coming into use. High-density edge QAMs are QAM modulators with multiple, contiguous RF channels being sourced by a shared upconverter via a common connector. DOCSIS downstream RF characteristics are all contained in the table named "CMTS Output" (Table 4-12 in ANSI/SCTE 22-1 2002 DOCSIS 1.0; Table 4-13 in ANSI/SCTE 23-1 2002 DOCSIS 1.1; Table 6-15 in ANSI/SCTE 79-1 2003 DOCSIS 2.0). The number of channels in a block served by a single upconverter should be reflected in the RF specifications in the updated "CMTS Output" table. In no case should the specifications reduce the requirements for a single channel CMTS. Instead, the specifications should be updated to reflect the more complex situation of power addition from the multiple RF sources contributed by a single upconverted block of channels including both spectrally aggregating and spectrally non-aggregating spurious and noise components.

5.1.2 Session and resource management architecture

To satisfy the desire for common resource management across all services/applications, a framework for session and resource management is necessary, as shown in Figure 17.

Figure 17. Session and Resource Management Framework



To increase efficiency in use of resources, the next generation head-end employs a session-based resource management architecture. Creation of such an architecture requires close control of the resources to ensure their efficient use. In an attempt to provide a generic framework, the session and resource management function is split into three domains: Application, Session and Resource Management. Each of these domains is discussed in detail in the following sections.

5.1.2.1 Application Manager

An Application Manager plays a coordinating role involving application signaling as well as interaction with the Head-End resource management framework via the Session Manager. In most cases the Application Manager is expected to be owned and operated by the cable operator. However, there may be cases where the Application Manager is in fact outside the cable operator's control. Examples of operator-hosted Application Managers would be VOD services and telephony services. Examples of third-party Application Managers could be streaming audio/video, and gaming services.

In a VoD system, it is the session manager's responsibility to maintain and manage the life cycle of session rather than the application manager. For such cases, the client can set up a session directly with session manager or proxy through the Application Manager. Since the Application Manager does not need to manage the session itself, this architecture allows for different applications to use the same session manager for multiple on-demand services.

For IP based applications and services, the typical implementation actually integrates the session manager into the application server; while they may reside in the same physical box, they are considered logically separate.

5.1.2.2 Session Manager

The role of a Session Manager is to broker head-end resource requests on behalf of the Application Manager. While an Application Manager only knows the QoS needs for the session, the Session Manager needs to understand how to translate those QoS needs into the various system resources as well as identify non-QoS based resources the session may also require (i.e. encryption resources, server resources). Since each operator network is expected to be a variation of the reference architecture, it is also the responsibility of the session manager to understand what resources are available in the system and choose the proper resources based on the specific applications needs.

To accomplish these tasks, the Session Manager needs to understand the system topology and all the resources that are available to a session and then determine which resources are appropriate. While a system may have numerous resources available, a basic service such as switched video will only need to take advantage of subset of those resources. In order to facilitate the Session Manager in determining the resources needed, the Application Manager provides application-identifying information in its request allowing the Session Manager to 'look up' the associated application resource needs. This frees the Application Manager to be unaware of the system topology and resources and to focus on managing applications and services.
It is important to note that multiple instances of a Session Manager may exist in a given head-end and each Session Manager communicates with a set of Resource Managers. The set of Resource Managers a Session Manager communicates with is

determined by the applications for which the Session Manager is expected to handle resource requests. Such an architecture allows for more rapid introduction of new services by not requiring a central 'super' Session Manager be upgraded every time a new service is trialed. It is envisioned that a given Application Manager will talk to a single Session Manager except where redundant Session Managers are implemented. Session Managers need not be able to support all session types; in fact, it is likely that separate Session Managers will be deployed for different types of sessions, e.g., VOD versus DOCSIS versus switched broadcast.

The Session Manager will not make business based policy decisions. Rather, it will coordinate application resource needs acting under the assumption that the request comes from a valid device and from a subscriber authorized to request such services. It may make resource based policy decisions based on the current status of the system resources, i.e. it may decide to reject a request if the resources are unavailable, or it may decide to pre-empt an existing session in favor of a new session.

5.1.2.3 Resource Manager

The Resource Manager deals primarily with allocating the resources necessary to satisfy a session request. Each head-end resource will have an associated (logical) Resource Manager. It is the Resource Manager's task to track all consumption of resources and allocate new resources as needed. Examples of Resource Managers are:

- On Demand Resource Manager – Streaming Server resources
- Encryption Resource Manager – Stream Encryption resources
- Network Resource Manager – Switched IP Network resources
- DOCSIS Resource Manager – DOCSIS MAC resources
- Edge Resource Manager – QAM resources
- Home Network Resource Manager – In Home Network resources

A Session Manager will translate and forward an Application Manager's QoS request to a given Resource Manager. The Resource Manager will then determine if the resources are available to grant the request and assign them if they are. For example, an Edge Resource Manager may get a request for a 3Mbps stream; if it has resources available to grant this request, it will tell the Session Manager which resource to use.

To further explain the Session and Resource Management Framework, the following two examples are provided:

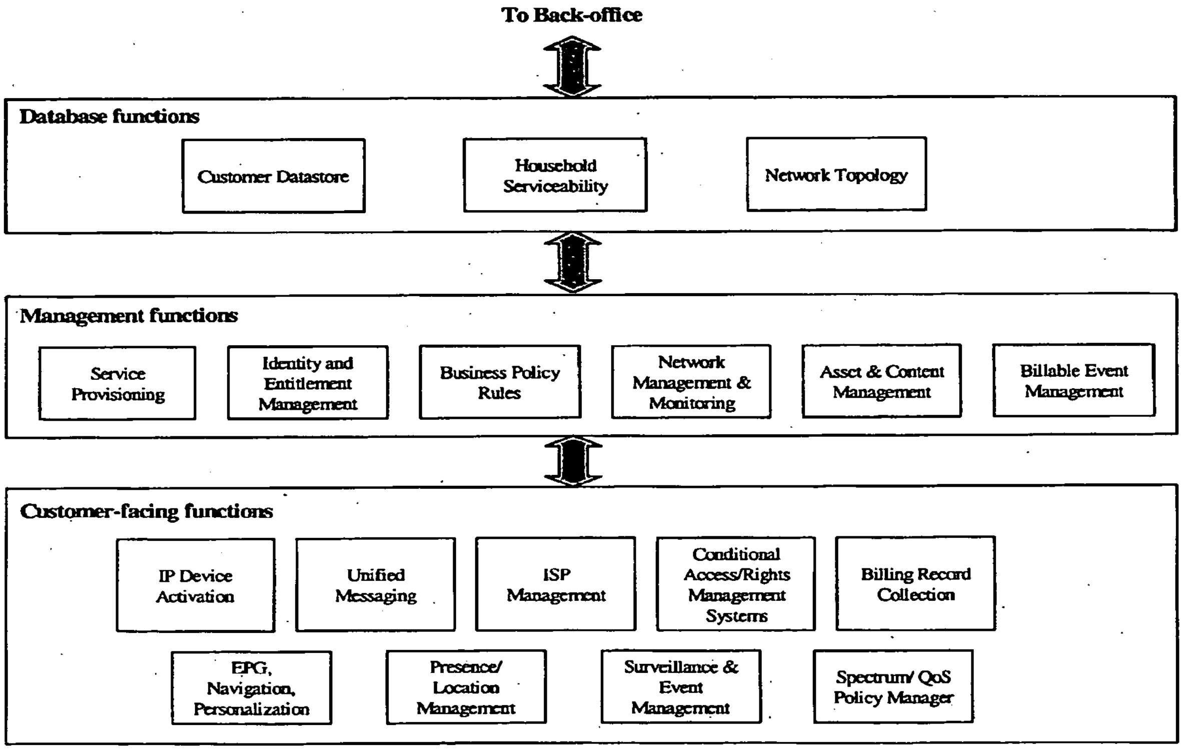
- When a CMTS (DOCSIS MAC) comes on line, its configuration will tell it how much bandwidth it should request. The CMTS will then make a request for edge QAM and Transport Network resources to satisfy its configured bandwidth. In this case the CMTS is acting as a combined Application/Session Manager and as such communicates directly with the resource managers.
- In contrast, a VOD service follows the following flow: The client starts the session by making a request for a VOD asset to the Application Manager. Upon receipt of such a request, the Application Manager will forward the request to the appropriate Session Manager who will then determine the overall resource requirements for the session. Once the session resources have been determined, the Session Manager will negotiate with multiple Resource Managers to obtain

the corresponding resources. These may include (not necessarily in any order) server resource, network resource, encryption resource, and edge resource. For example, the edge resource allocated may be dependent on the required bandwidth and service group the client belongs to. The server resource allocated may be determined by where the VOD asset is located. And the network Resource Manager will determine a network path from the server to the edge.

5.2 Head-end management architecture

This section relates to head-end management partitioning and information, as well as evolution of the video provisioning architecture. To support the management and control of the head-end servers and content sources, Figure 18 shows a reference architecture for the management and information technology components.

Figure 18. Head-end Management Architecture


To Back-office
Database functions
Customer Datastore
Household Serviceability
Network Topology
Management functions
Service Provisioning
Identity and Entitlement Management
Business Policy Rules
Network Management & Monitoring
Asset & Content Management
Billable Event Management
Customer-facing functions
IP Device Activation
Unified Messaging
ISP Management
Conditional Access/Rights Management Systems
Billing Record Collection
EPG, Navigation, Personalization
Presence/ Location Management
Surveillance & Event Management
Spectrum/ QoS Policy Manager

As shown in Figure 18, the head-end management architecture includes customer-facing functions, management functions, and database functions.

As an example of a *customer-facing function*, ISP Management provides for email, personal web pages (PWP), and portals; it supports management of subscribers' ISP accounts, cross-selling of services via the web pages, and interfaces for communities and subscriber interactions for games or other activities.

Examples of *management functions* include:

- **Service Provisioning** for subscribers via internal systems and via external third-party systems, e.g., to support local number portability and/or complementary services.
- **Business Policy Rules** that set priorities for different kinds of traffic and for different relationships with third-parties, and that support marketing and bundling initiatives. These rules may derive not only from cable operators but also from their content or service providers.
- **Billable Events** that rate transactions and calculate charges to subscribers or partners such as advertisers.

Interfaces between the head-end information technology (IT) infrastructure and back office systems are affected by means of shared (or replicated) databases between the head-end and back-office IT systems. Examples of *database functions* include:

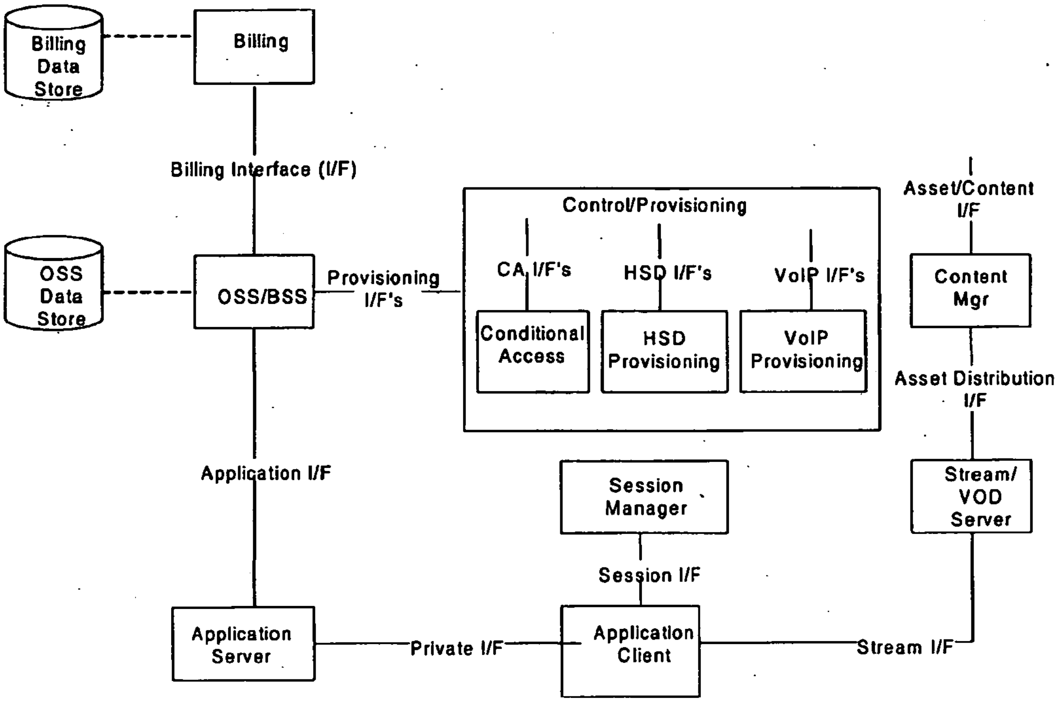
- **Customer Datastore** maintains customer identities, and stores information on the services and CPE associated with specific customers.
- **Household Serviceability** maintains information on availability of services and capabilities associated with locations, such as high-speed data, telephony, or high-definition TV. Such information may be made available to retailers, perhaps through Go2Broadband, to support retail distribution channels for cable equipment and services.
- **Network Topology** maintains information on network attributes such as strand maps, fiber counts to fiber nodes, GigE network facilities, multiplexers and/or dedicated fibers to business customers, and wireless network extensions via strand-mounted WiFi access points.

5.2.1 Head-End Management Partitioning and Information Architecture

Figure 19 represents an instance of head-end management functions covered above, and identifies eight specific functional partitions that participate in delivery of service to subscribers. This instance diagram and the information model to follow are represented for the purposes of identifying a subset of information and interface requirements for the purposes of standardization.

This presentation suggests a mid-term solution to alleviate restrictions in accessing the back office billing system. Longer-term solutions may also evolve that will affect access to billing system data and functions.

Figure 19. Head-End Management Partitioning and Interfaces



Each component in Figure 19 is defined below.

- **Billing**

The billing system is responsible for billing end subscribers, and for many operators, for participating in customer care subscriber management functions. The billing system is the system of record for subscriber data, and billable services.

- **OSS/BSS**

The OSS/BSS is responsible for evaluating business rules, and transacting the functions of (or responding to) other subsystems. The OSS/BSS will be responsible for interfacing with the following systems:

- Billing system to propagate purchases such as VOD/PPV purchases and call detail records, as well as to synchronize subscriber and product catalog data.
- Application Server systems to provide a single point of interface for requests for services. Generally these requests include eligibility and fulfillment requests.
- Provisioning/Control systems to perform provisioning and control functions, such as conditional access or modem provisioning.

OSS/BSS functions are performed by a conglomerate of subsystems, but will coordinate functions through workflow, and act on locally persisted data. Subsystems will perform functions such as:

- Entitlement Management
- Identity Management
- Product Offering Management
- Purchase Management
- Application Management
- Topology Management

- **Control/Provisioning**

Control and Provisioning systems are responsible for communicating with head-end equipment and subscriber devices to deliver service. Control systems include:

- Conditional Access Controller manages the encryption of MPEG transport, as well as device access to those transports.
- IP/Device Provisioning is responsible for (IP) address assignment and configuration download to specific devices.
- VoIP Softswitch Provisioning manages VoIP telephony signaling, mapping device endpoints to telephone numbers and their associated telephony features (e.g. call waiting).

- **Session Manager(s)**

The Session Manager(s) are responsible for setting up sessions for clients to designated end-points at a specific quality of service (bandwidth). Sessions will be established based upon requests from clients. For more details, see the section on Session and Resource management architecture.

- **Streamer/Video Server**

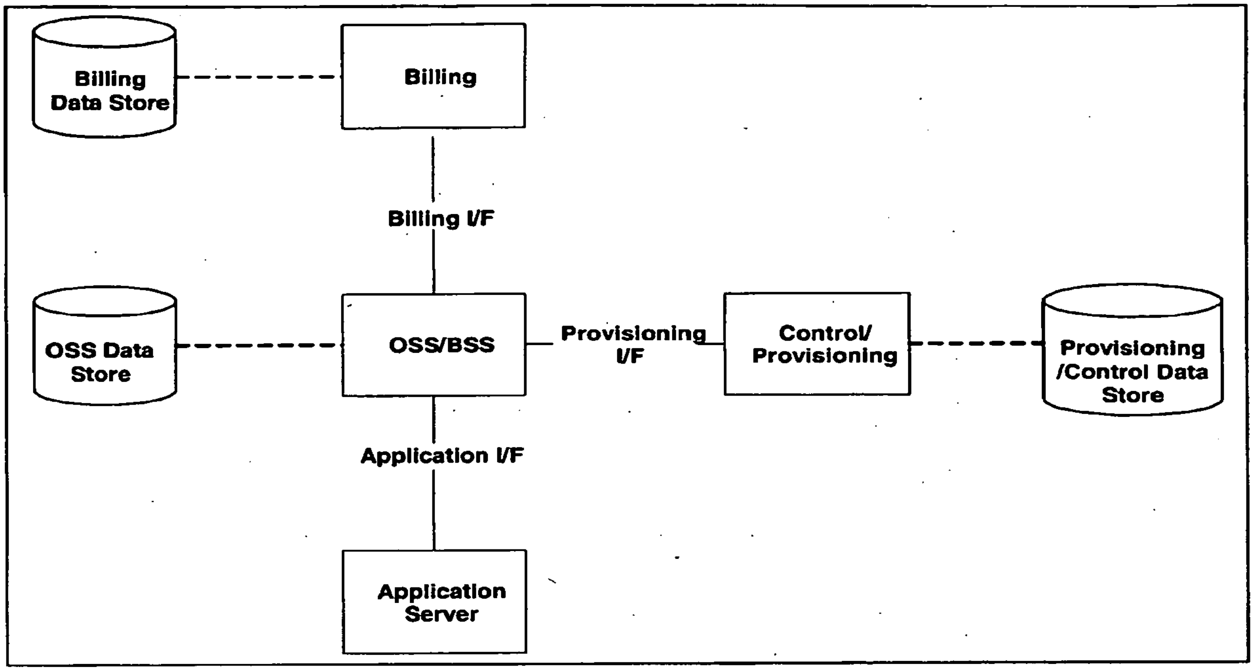
The streamer/video server is responsible for streaming content to clients. Many include embedded/attached storage, and are responsible for receiving content from content providers for storage on the operator platform.

- **Content Manager**

Content Managers are responsible for managing content and metadata on the operator network, and controlling the distribution and propagation of content and metadata to systems within the operator platform.

Figure 20 represents a simplified view of the data needs at significant established management system boundary points within the NGNA architecture. The diagram is not intended to be a complete representation of all data or boundary points within the network, but only those associated with service delivery and fulfillment, and then again, only those that are established across all MSO platforms.

Figure 20. Simplified Head-End Management Datastores



The three database symbols on this diagram represent persistent data stores required by the billing platform, OSS/BSS, and Control/Provisioning systems respectively.

Billing System Information (Persisted Data)
The billing platform will maintain the following information, and is considered the system of record for subscribers, equipment as a capital asset, and billing codes.

Household
- Attributes: physical service location, franchise area, fibernode
- "Household ID" is household-centric: billing system id (corp or sys-prin) + house + customer

Customer
- "Customer ID" associated with a customer
- Attributes: name, phone, billing status, billing address

Equipment
- Associated with Household/Outlet
- Attributes: make, model, serial number, MAC address(es), outlet, service/rate codes

Service/Rate Code
- Associated with billing system id (e.g. corp or sys-prin)
- Attributes: type, price, promotion, reporting center(s)

Work Order

- Associated with Household
- Attributes: job type/status/dates, outlets, service/rate code changes

OSS/BSS Information (Persisted Data)

The OSS/BSS management system will maintain the following information and is considered the system of record for entitlements, specific subscriber identity, network provisioned or assigned information such as IP addresses.

Customer

- Represents account to which one or more services are supplied
- Maintains associations to equipment of the customer
- Maintains associations to entitlements of the customer

Equipment

- Logical Device Data
- Physical Device Data
- Includes network specific information
- Maintains association to entitlements

Service Definition (Entitlement Mapping)

- Video Services
- HSD Services
- VoIP Services
- Identifies specific provisionable activities

Service Offerings/Product

- Data for presentation to user
- Association with entitlements
- Association with billing codes

Entitlements

- Entitlement ID for every service subscriber is authorized for

Billing System Product Mappings

- Maps rate codes to service definitions for provisioning

Control/Provisioning Systems Information (Persisted Data)

The Control/Provisioning management system will maintain the following information and is considered the system of record for provisioned data necessary to fulfill requests via the OSS/BSS system above, and is dependant upon the type of provisioning/control system considered.

- **Equipment**
  - Logical Device Data
  - Physical Device data
  - Specific control/provisioning system attributes
    - IP Addresses
    - Conditional Access Entitlements

- Mailboxes

- **Services**
  - Specific control/provisioning system attributes
    - IP Addresses
    - Conditional Access Entitlements
    - Modem config files
    - Assigned numbers

- **Service Management Interfaces**

The following interfaces are under consideration for standardization.

- Billing Interfaces
- Conditional Access Interfaces
- Application Interfaces

- **Billing Interface**

The interface between the billing system and the operator head-end management systems (OSS/BSS in the diagram above) system will focus on the following functions:

- Household functions (such as determining serviceability, or finding customers)
- Account/Customer Management functions (such as finding a customer, or processing a purchase)
- Financial functions (such as running a credit card, or processing EFT)
- Equipment Functions (such as getting equipment associated with a household or subscriber, or propagating equipment purchases)
- Product Offering Functions (such as determining offerings available for a specific customer/equipment)
- Discount, promotions, campaign functions (such as determining discounts specific to specific offers)

This interface is fully bi-directional (meaning either side of the interface can initiate transactions) and transactional.

- **Provisioning/Control System Interface**

While there are several interfaces that should be considered here, the conditional access interface will be considered in more depth. The conditional access interface provides the head-end management system (OSS/BSS in diagram above) to initiate the encryption of any MPEG transport streams. The interface will also result in the generation of ECM's and EMM's. Interfaces will provide both raw and service oriented functions.

- Service creation functions, with resultant entitlements
  - Single continuous linear service (single premium channel subscription)
  - Multiple continuous linear services (package or tier)
  - Time limited linear services (ppv event)
  - Multiple time limited linear services (ppv package)
  - Instantaneous non-linear service (VOD, asset based)
  - Multiple mixed services (all of the above)

- Enable/Disable device
    - Enable device for entitlement
    - Disable device for entitlement

- **Application Interfaces**

The application interface identifies a subset of services specific to video oriented applications.

- Access to offering data
- Access to subscriber/identity data
- Access to equipment data
- Validate/check eligibility
- Initiate session
- Make purchase of an offering

5.2.2 Evolution of the Video Provisioning Architecture

Figure 21. Video Provisioning Architecture

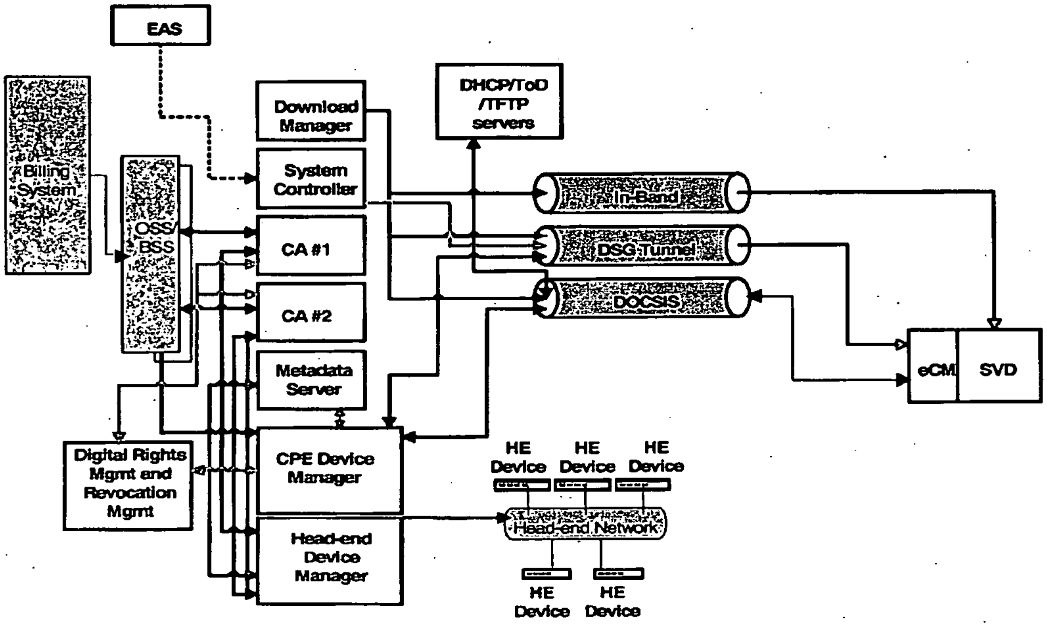


Figure 21 describes the intended path for two-way and unidirectional communication between a CPE device and the head-end. Note that video traffic is not represented here.

DSG Tunnel: The DSG Tunnel is managed by CMTS configuration, in coordination with the rest of the video provisioning systems. In addition, DHCP, ToD and TFTP servers are necessary to support DOCSIS-enabled settops.

Download Manager: The Download Manager configures, controls and monitors downloads to CPE devices. OpenCable Common Download would be supported by this component. The Download Manager can support downloads over the DSG tunnel, DOCSIS, or In-Band. The Download Manager should provide an interface to the CPE Device Controller so that channel maps, resources, etc. can be modified to support the necessary code objects. There is a very secure component of the Download Manager that enables the encryption and secure download of the conditional access system firmware.

System Controller: The System Controller handles such things as System Information, EAS, and System Time. The System Controller implements open standards for communication to CPE, i.e. SCTE-18 for EAS and SCTE-65 for Channel Map and Video Network configuration.

CA Controller: The CA Controller handles only Key Management and Authorization. It interfaces with the operational support system (which in turn interfaces with the CPE Device Controller) and the Head-end Device Manager to deliver keys and authorizations for video services. The CA Controller interfaces with the CPE and Head-end Device Controllers to deliver EMMs and ECMs.

Metadata Server: A typical cable system today has multiple sources of Metadata. This component will be a single source of metadata for everything from guide data delivery to encryption device delivery. A single source of metadata allows a change to be propagated throughout the entire system by making a change in a single place. VOD Metadata may still need to be separated from the Metadata server, since VOD events are unique to the VOD server.

CPE Device Manager: The CPE Device Manager delivers configuration information, parameters, and features, to a CPE Device. It requests authorizations (EMMs) from the CA Controller and forwards them on to the CPE. All other functionality for CPE devices is handled here. The CPE Device Manager will interface with the Session and Resource Management system to control on-demand session set-up.

Head-end Device Manager: The Head-end Device Manager is a component that monitors, controls and configures all head-end equipment in a system. It also handles encryption schedules by interfacing with the CA Controller. This is done over the IP network at the head-end – the devices that are managed by the HDM are encryption devices (i.e. IRTs), modulators, upconverters, etc. The HDM should also interface with the resource managers and the QAMs.

Digital Rights Management and Revocation Management: These components configure CPE devices for DRM Support, and interface with the CA Controller when necessary.

5.2 Applications Performance Management

As cable operators offer increasingly sophisticated, interactive services there will be an increased desire to monitor the experience of subscribing end-users for each application, in addition to traditional infrastructure and plant surveillance. Such monitoring, which will occur remotely at the operator's head-end or other network operations center (NOC), will apply to technical performance and will not provide any information for non-technical purposes that may have privacy implications.

Desirable features of this performance monitoring layer include:

- CPE includes the ability to monitor and collect performance and trouble data while offline. This allows for trouble data to be accumulated during periods when connectivity may fail and also distinguishes between an offline device (powered off) and one that is simply unable to connect. It also provides for better scalability than a centralized approach.

- Thresholds set to detect critical performance issues and send alarms to a NOC. This requires a facility to be implemented that produces SNMP "traps" or similar alarms.

- Thresholds set to detect minor performance issues and send periodic summary reports to a NOC (on the order of once/day).

- Alarms that uniquely identify the device/user.

- The ability to embed or download a performance monitoring application (PMA) for each user application (e.g. iTV, program guide, pay per view, web surfing, email access, etc). A PMA would be downloaded based on a class of the application to monitor.

- The ability for the PMA to register for details regarding flows of traffic, and to be delivered messages indicating timestamps and protocol headers (exact fields are a function of the class of application/protocol). Timestamps should be accurate to within 1/100 of a second. Flows should be based minimally on IP port number and/or destination IP address.

APPENDIX A

A. Glossary

1394	IEEE 1394, also called Firewire
AAA	American Academy of Advertising
AAAA	American Association of Advertising Agencies
AC-3	Audio coding standard developed by Dolby Labs
AES	Advanced Encryption Standard
ANA	Association of National Advertisers
API	Application Programming Interface
ASD	Authorized Service Domain
A-TDMA	Advanced Time Division Multiple Access
ATSC	Advanced Television Study Committee
AVC	Advanced Video Coding
BP	(CableHome) Boundary Point
BPI+	DOCSIS Baseline Privacy Plus
CA	Conditional Access
CAB	Cable Advertising Bureau
CAS	Conditional Access System
CAT	Conditional Access Table
CBC	Cipher Block Chaining
CBR	Constant bit rate
CCI	Copy Control Information
CE	Consumer electronics
CMTS	Cable modem termination system
Codec	Coder/Decoder
CORBA	Common Object Request Broker Architecture
CPE	Customer premises equipment
CRL	Certificate revocation list
CSA	Common Scrambling Algorithm
CW	Control Word
DES	Data Encryption Standard
DFAST	Dynamic Feedback Arrangement Scrambling Technique
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services Architecture for Network Traffic
DHWG	Digital Home Working Group
DLNA	Digital Living Network Alliance
DOCSIS	Data Over Cable Service Interface Specification
DRM	Digital Rights Management
DSCP	DiffServe Code Point
DSG	DOCSIS Set-top Gateway
DSM-CC	ISO/IEC Digital Storage Media – Command and Control
DSP	Digital signal processing
DSS	Digital Signature Standard
DTCP	Digital Transmission Content Protection
DTV	Digital TV
DVB	Digital Video Broadcast
DVI	Digital Video Interface
DVR	Digital video recording

ECB	Electronic Code Book
ECM	Entitlement Control Message
ECPA	Electronic Communication Privacy Act
EMC	Electromagnetic compatibility
EMM	Entitlement Management Message
EPG	Electronic program guide
FIPS	Federal Information Processing standard
FPGA	Field Programmable Gate Array
GigE	Gigabit Ethernet
GSD	Guaranteed Service Domain
HAVI	Home Audio Video Interoperability
HDCP	High-bandwidth Digital Content Protection
HDMI	High definition multimedia interface
HDTV	High definition TV
HFC	Hybrid fiber coax
HPNA	Home Phoneline Networking Alliance
HSD	High speed data
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDR	IP Data Record
J2EE	Java Two Enterprise Edition
KEK	Key Encryption Keys
Layer 2	Link layer in Open Systems Interconnection (OSI) framework
Layer 3	Network layer in OSI stack; Layer in firewall in which routing is based on IP address.
LDAP	Lightweight Directory Access Protocol
LEC	Local exchange carrier
Low-Split	Common HFC frequency assignment in which upstream (to head-end) is below 42 MHz and downstream (to customer) is above 54MHz.
L/R	Left/Right baseband audio outputs from stereo system
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
Mid-split	Proposed upstream/downstream cross-over point between 85MHz-105MHz to increase available upstream bandwidth.
MoCA	Multimedia Over Coax Alliance
MPEG	Motion Picture Experts Group
MPTS	Multiple Program Transport Streams
MTA	Multimedia Terminal Adapter
NAT	Network address translation
NCS	Network Call Signaling
NCSP	Next generation configurable security processor
nDVR	Network DVR
NE	Network elements
NGNA	Next Generation Network Architecture
NIU	Network Interface Unit
OCAP	OpenCable Applications Platform
OEM	Original equipment manufacturer
ODRL	Open Digital Rights Language Initiative
OOB	Out of band

OSS	Operations Support System
PC	Personal computer
PERM	Protected Entertainment Rights Management
PES	Program Elementary Stream
PHY	Physical layer
PID	Packet Identifier
PMA	Performance Monitoring Application
PS	Portal services
PSI	Program Specific Information
QAM	Quadrature Amplitude Modulation
QoS	Quality of service
QPSK	Quadrature phase shift keying
RAN	Regional area network
RMS	Rights Management System
ROSI	Return on security investment
RSA	Public key cryptosystem developed by Rivest, Shamir, Adleman; also company by same name marketing public key technology.
RSVP	Internet protocol to reserve resources for streaming content QoS
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
S-CDMA	Synchronous Code Division Multiple Access
SCTE	Society of Cable Television Engineers
SD	Secure Digital
SDM	Sub-band Division Multiplexing
SHA-1	Secure hash standard #1
SIP	Session Initiation Protocol
SNMP	Simple network management protocol
SOAP	Simple object access protocol
SOC	System on a chip
SPTS	Single Program Transport Streams
SVD	Subscriber video device
S-Video	High quality video interface, derived from Super VHS signal format
TFTP	Trivial File Transfer Protocol (Trivial FTP)
ToD	Time of day
TOS	Type of Service (also DiffServ Code Point, DSCP)
TCP	Transmission Control Protocol
TS	Transport stream
UDCP	Unidirectional Digital Cable Product
UDP	User Datagram Protocol
UI	User interface
UPnP	Universal Plug and Play
USB	Universal serial bus
VBR	Variable bit rate
VLAN	Virtual Local Area Network
VSB	Vestigial SideBand
VOD	Video on demand
VoIP	Voice over IP
XML	Extensible Markup Language
XrML	Extensible Rights Markup Language

APPENDIX B

B. Requirements

Certain requirements have been taken into account in considering next generation network options. These requirements include the following:

Expanded Capacity

As cable operators add new services, demands for network capacity continue to increase. The next generation network needs to support expanding requirements for video program services, including high-definition services; on-demand video services; high speed data services involving enhanced downstream data rates and symmetrical upstream capacity; and IP multimedia services. Sufficient capacity is necessary for foreseeable downstream and upstream applications, tools are necessary to manage available capacity efficiently, and low cost means are necessary to add capacity as required.

Solutions based on open standards

Non-proprietary solutions are preferred as a means to ensure interoperability of equipment from multiple suppliers, to allow greater vendor participation in the market, to reduce cost, to increase innovation, and to support retail sale of customer premises equipment. It is desirable that interfaces be based on existing open standards wherever they apply and in areas lacking existing standards, it will be desirable to create open standards. It may be necessary to provide extensions to existing standards as long as the extensions are open.

Exploit existing assets

One objective is to expand available capacity to meet anticipated service requirements within the current typical cable system bandwidth up to 750MHz for downstream transmissions. The next generation network should continue to support multiple existing legacy assets, e.g., digital set-top boxes that use proprietary conditional access and out-of-band signaling. Network objectives should be achieved without additional rebuilds of cable outside plant or stranding of legacy subscriber CPE (customer premises equipment).

Secure rights management

Secure rights management of valuable content encourages expanded participation by content providers in cable-provided services and supports introduction of innovative new services and new business models. Content needs to be protected as it is networked among cable-managed devices in subscriber households.

Network resource sharing

The next generation network needs to share network resources across services to enhance efficiency in the use of cable network assets. For example, QAM resources can be shared with dynamic provisioning by different services.

Managed subscriber devices

Home networks for video, data, and interactive multimedia services represent an important component of the next generation network. For example, media servers will be sharable across multiple home devices including subscriber video devices and Internet appliances. Further, to enable cost-effective configuration, provisioning and management of the widest variety of possible CPE devices in subscriber households, these devices need to support automatic discovery and remote monitoring and control. Remote monitoring includes both the health of the device as well as the health and performance of the individual services that the CPE supports or transits. To accommodate potential new arrangements with third-party transaction or content providers, it is also desirable for CPE to enable usage accounting. It is also desirable to provide performance monitoring and exception alarming on a service-by-service basis, and build on and extend elements defined in the CableHome project.

Cable competitiveness
One requirement for the next generation network is to enable cable operators to differentiate their services, or at minimum ensure competitive parity, in terms of features, functions and cost, versus offers from digital DBS providers, telephone companies and other competitors.

Scalability
The next generation network should be capable of cost-efficient growth to support additional services, new subscribers and/or increased simultaneous usage of on-demand and interactive services. The architecture also should be able to scale "down" to work cost-effectively in smaller systems.

Flexible service delivery
Cable operators require flexibility to rapidly provision and support new services with equipment, features, and pricing tailored to the disparate needs of the wide range of subscriber households. Such new services may involve different business models than those currently offered.

Operators also need flexibility for cross-service promotions, for example to be able to offer free movies for upgrading data service.

The next generation network is a platform for launching many new services and should be easily extensible to add such services without stranding earlier investments.

The next generation network also should accommodate new compression and transmission standards, for example allowing cost-efficient evolution from currently-deployed MPEG2 video compression to standards offering equivalent video quality at much lower bit rates.

Alignment with external technology
The next generation network should exploit the technologies that will most benefit from continued innovation and cost reductions, for example, the continuing gains in digital signal processing, memory, and optical communications systems.

Support for retail sale of cable CPE
The next generation network expands consumers' choices of CPE, including retail purchase of consumer electronics, PCs, and other devices that could connect to cable networks directly or indirectly. Such devices should work seamlessly in providing cable services along with MSO-provided CPE, in accordance with agreements between the cable industry and consumer electronics manufacturers, and with FCC regulations.

Minimize operations burden
It is anticipated that in many cases the next generation architecture should reduce cable operators' operational cost and complexity, limiting additional or complex tasks for field operations or back-office personnel.

Support for authorized third-party use
Cable TV systems currently serve as channels for third-party content providers under distribution agreements with the cable operators. The next generation network's increased capacity and capabilities will expand cable operators' opportunities to partner with third-party content and transactions providers. It is important that the next generation network provide the means for cable operators to encourage and support authorized uses, including authorized third-party use, while protecting the cable network from unauthorized third-party uses that may disrupt, impede or impair the authorized services offered to cable subscribers.

Satisfy Performance criteria
The next generation network should satisfy quantitative performance criteria in terms of capacity, reliability and latency for the services or applications carried by the network, such as in terms of measurable Service Level Objectives and Service Level Agreements.

Alignment with MSO financial objectives
The architecture and interfaces should be implemented in a cost-effective manner, based on commodity and/or specialized hardware and software as long as they are cost-effective.

Investments in next generation network equipment should result in near-term financial benefits such as improved operating efficiencies and/or growth in profitable subscriber revenue.

Current cable networks need to migrate cost-effectively to the next generation architecture. "Cost effective" migration implies avoiding stranding existing assets. It also implies that the types of investments -- fixed versus variable, integrated versus modular -- are aligned with the nature of the market opportunities and subscriber environments in which the investments are made.

APPENDIX C

C. Security

Details on specific aspects of the NGNA security system are provided in this appendix.

C.1 Security Hardware Element

The Next generation Configurable Security Processor (NCSP) hardware element supports the following standardized algorithms for transport stream encryption at the head-end and decryption at the CPE:

- Data Encryption Standard (DES) - Electronic Code Book (ECB), Cipher Block Chaining (CBC) and other modes for residual blocks [Federal Information Processing standard, FIPS 46-2]
- Triple DES – ECB, CBC, and other modes for residual blocks [FIPS 46-2]. This includes support for both two-key and triple-key encryption.
- Advanced Encryption Standard (AES) (Rijndael)
- DVB - Common Scrambling Algorithm (CSA)

The NCSP hardware element is configurable ("renewable") and employs technologies to support the decryption of at least the following five types of secure transport streams:

1. DigiCipher II – as defined and licensed by Motorola.
2. PowerKey – as defined and licensed by Scientific-Atlanta.
3. Triple DES – supporting ECB and CBC at a minimum as well as two-key and three-key modes.
4. DVB-CSA – as defined in DVB.
5. AES – using a new standardized key architecture with standardized ECM, EMM, unit seed, and unit ID methodology.

Note that the NCSP is defined in such a way that silicon providers will not be required to obtain DigiCipher^{TM} or PowerKey^{TM} licenses in order to build NCSP functionality into their products. The NCSP is defined in a manner such that compliant silicon will be able to run the appropriate algorithms that are downloaded to the NCSP when connected to the cable plant.

C.2 Authentication

The hardware components of the NCSP should be capable of securely storing and performing digital signatures using various sizes (1024, 2048 and 4096-bit) of RSA keys in hardware registers. The next generation components should be capable of securely generating digital signatures inside tamper resistant hardware without exposing the private keys or the processing needed to generate the hash, and encrypt. The next generation network should be capable of digitally signing messages used for authentication and providing integrity using a secure SHA-1 hash.

C.3 Key Encryption Keys (KEK)

NCSP hardware should be capable of securely storing Key Encryption Keys which could be in the form of symmetric or, preferably, asymmetric cryptography. The ability to use key pairs for transporting encrypted keys among CPE devices and to head-end devices is very desirable.

C.4 Unit Address

Each NCSP used in a CPE device should be uniquely identified with a completely unique ID. This ID is used to address each CPE device for receipt of the entitlements for that specific CPE device. In some implementations, a MAC address may be used for this ID.

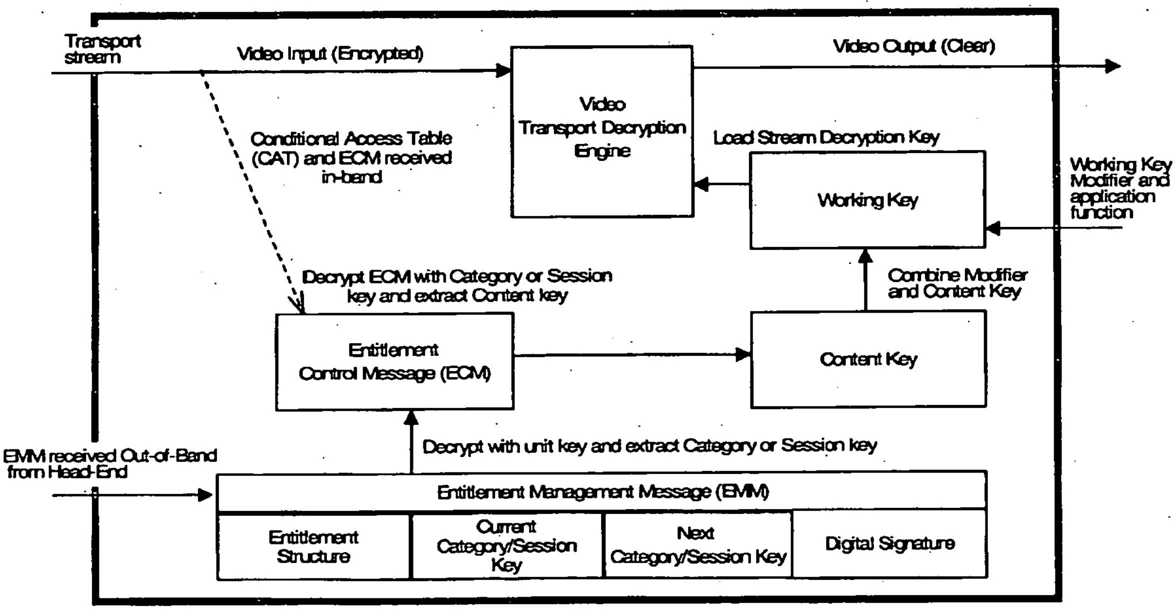
C.5 Tamper Resistance

The NCSP is designed to meet FIPS-140 Level 2 security in most areas with some areas (hardware re-configuration and firmware upgrades) requiring FIPS 140-2 Level 3 security. It also employs the latest technologies (for example, power plane distribution and cell fragmentation) in tamper resistance to prevent electron microscope analysis and surface shaving attacks.

C.6 Key Management

The key hierarchy includes multiple keys as illustrated in Figure 22.

Figure 22. Key Hierarchy


Transport stream
Video Input (Encrypted)
Video Output (Clear)
Video Transport Decryption Engine
Load Stream Decryption Key
Working Key
Working Key Modifier and application function
Conditional Access Table (CAT) and ECM received in-band
Decrypt ECM with Category or Session key and extract Content key
Combine Modifier and Content Key
Entitlement Control Message (ECM)
Content Key
Decrypt with unit key and extract Category or Session key
EMM received Out-of-Band from Head-End
Entitlement Management Message (EMM)
Entitlement Structure
Current Category/Session Key
Next Category/Session Key
Digital Signature

The NCSP software and hardware is designed to employ new concepts and technologies in the area of key management while functioning with existing legacy systems using key sharing or re-configuration criteria. Decrypted keys extracted in the CPE from the video stream and ECMs and EMMs should be loaded directly into the decryption engines without passing over external interfaces including the transport decryptors.

C.6.1 Entitlement Control Messages (ECMs)

An ECM is an encrypted message that contains access criteria to various service tiers and a Control Word (CW). The Control Word is the seed key that is modified and used to decrypt the video stream and should be able to be changed on a variable periodicity or in effect converted into a "working key." The ECM is decrypted and checked in the CPE against the access criteria in order to provide authorization. If authorization is granted, the CW will be released, converted to a working key and used to decrypt the content at the CPE device.

C.6.2 Entitlement Management Messages (EMMs)

Encrypted messages are created in the head-end and sent to the next generation CPE to authorize the CPE device for certain access criteria to content. The EMM contains the actual authorization data and should be sent in a secure method to each CPE device. The EMM is addressed to a single CPE device and is uniquely encrypted so that only that device can decrypt the entitlements and validate them. The NCSP should support DigiCipher II, PowerKey, NDS, Nagravision, and NCAS entitlement mechanisms and formats.

C.7 Copy Protection

If an NGNA device employs a CableCARD, the interface should implement renewability and configurability in compliance with SCTE-41. In addition to supporting the current SCTE-41 transport stream requirements, NCSP should be capable of decrypting the following three types of secure transport streams:

1. Copy Protection - DES (as defined in SCTE-41, with the additional option of using DES CBC mode in addition to EBC mode).
2. Triple DES – supporting ECB and CBC at a minimum.
3. AES – using a new standardized key architecture with standardized ECM, EMM, Key Encryption Keys, and unit ID methodology.